Book 3 - Legal Aspects of Digital Forensics

1. Introduction to Law and Legal Systems

Scope	
Number	1
Title	**Introduction to Law and Legal Systems**
Introduction	This chapter provides a general, yet, concise overview of the Jordanian legal system, and how cyberspace relates thereto, in simplistic terms, it explains the structure of the Jordanian legal system, the hierarchy of legislation starting from the Jordanian Constitution, the major topics covered therein and how cyberspace is related.
Outcomes	The students will be able to understand the following: - The structure of the legal system and how laws function - Several basic legal concepts, especially the concept of law and legal rules and the different categories of legislation and the effects thereof. - How cyber issues are addressed in the legal system, at all stages and tiers. - The basic concepts of the criminal legal system, as a premise to the following chapters.
Topics	**Foundation of the Legal System** **Hierarchy of Legislation** 1. The constitution 1.1 Legislative Authority - Cyberspace and the Legislative Authority 1.2 Executive Authority - Cyberspace and the Executive Authority 1.3 Judicial Authority - Cyberspace and the Judicial authority 1.4 Fundamental rights and duties of Jordanians - Cyberspace and constitutional rights 2. International Treaties and Conventions - Cyberspace and International Treaties 3. Laws 4. Regulations (by-laws) 5. Instructions and decrees **Cyberspace and the law** 1. Private Law vs. Public Law 2. Criminal Law vs. Civil Law 3. Cyberspace in criminal law: cybercrimes 3.1 Misdemeanors vs. Felonies 3.2 Crimes against individuals vs. Crimes against property
Study Guide	

Task	Time
Preparation (Introduction and On-line Planning):	1.5 hrs
Textbook Content:	4 hrs
Thinking (online discussion review questions)	1.5 hrs
Tutorial Work on Law and Legal Systems	1.5 hrs

	Related Course Work	1.5 hrs
	Total	10 hrs
	Required external resources: - The Jordanian Constitution, - Alkhatib, Noman Ahmad; Political Systems and Constitutional Law; first edition; Dar Althaqafa Publication and Distribution; 2006, Amman; Jordan - UN, Department of Economic and Social Affairs (DESA); Hashemite Kingdom of Jordan Public Administration Country Profile; Division for Public Administration and Development Management (DPADM) United Nations; February 2004.	

Chapter 1 Introduction to Law and Legal Systems

Author **Lina Abdallah Khalil Shabeeb,**
Associate Professor of Public Law, School of Law, University of Jordan

Section Number 1 (Introduction to Law and Legal Systems)

Section Title **Foundation of the Legal System**

Introduction This chapter provides a general, yet, concise overview of the Jordanian legal system, and how cyberspace relates thereto, in simplistic terms, it explains the structure of the Jordanian legal system, the hierarchy of legislation starting from the Jordanian Constitution, the major topics covered therein and how cyberspace is related.
Note: The Jordanian legal system is very similar to the Palestinian legal system, therefore, this chapter will be based on the former, with references to the latter (where needed).

Content Law is one of the most important aspects that govern our lives today. It can be simply defined as "the system of rules which a particular country or community recognizes as regulating the actions of its members and which it may enforce by the imposition of penalties" (as defined by the Oxford dictionary).
Legal rules are considered (i) abstract and general rules applying to all members of the community without any discrimination of whatever nature; (ii) social rules governing the conduct and behavior of individuals; and (iii) obligatory rules accompanied by penalties and sanctions thus guaranteeing its proper implementation.
In Jordan the term law is used to refer to two related, yet different concepts, law in a general setting means binding rules, regardless of its source or power; however, in a technical legal setting, law refers only to the laws that are passed by the Jordanian Parliament, ratified by the King and promulgated in the Official Gazette (Article 93 of the Jordanian Constitution, and Articles 41, 70 and 116 of the Palestinian Basic Law for the year 2003). This is important if we take into consideration that the use of the term law could be – sometimes – misleading, especially since the law, passed by the Parliament, is superior, in the legislative hierarchy that the regulations, as will be illustrated hereunder.
The term legislation, however, refers to all written rules provided in the hierarchy of legislation.

Content

Section Number 1 (Introduction to Law and Legal Systems)

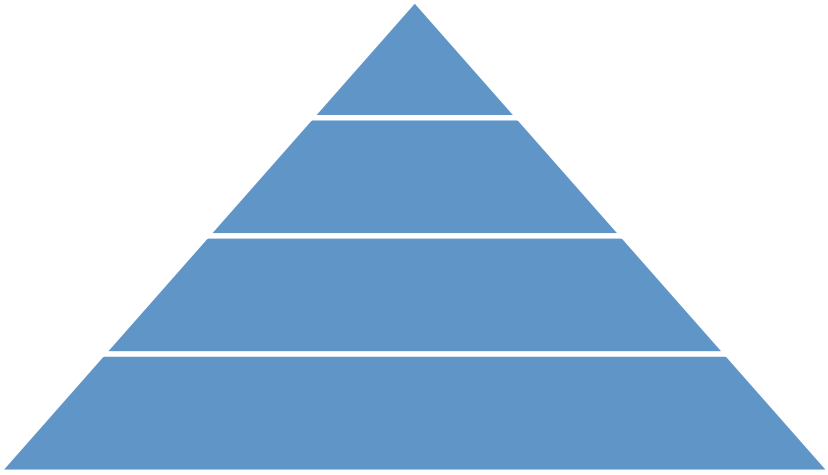
Section Title **Hierarchy of Legislation**

Introduction Due to the complex human interactions occurring nowadays, it is hard to limit the rules that govern such interactions. Therefore, each state establishes the most appropriate legal system in order to regulate the conduct and interactions of its individuals. Such legal rules vary in terms of its importance and in priority of implementation on one hand and in terms of the authority issuing such legal rules on the other hand. As such, a hierarchy of rules is evident in all legal systems.

Content The hierarchical structure varies from country to country and depends on the form of government. However, there are general principles that are common to most countries and are keys to determining the purpose of each piece of law within a legal and regulatory framework, and ultimately enforcing their authority and validity (Clegg, M., 2016, p. 4).
The Jordanian hierarchy of legislation is as follows:
- Constitution;
- International treaties and conventions;
- Laws;
- Regulations;
- Instructions and decrees.

To illustrate, all the legislation in this hierarchy encompass binding rules, however the higher the legislation is in this hierarchy, the more binding. Hence, a law cannot provide a rule that contradicts with the rules set by the constitution, and the

regulations cannot provide a rule that contradicts with either the law or the constitution, consequently, the instructions cannot contradict any other legislation.



CONSTITUTION
LAWS
REGULATIONS (BYLAWS)
INSTRUCTIONS

Figure (1): Pyramid of Legislation
* note that the international conventions are not added to the pyramid because they were added by courts' decision rather than the Constitution

1. **The constitution**

The constitution tops the Jordanian hierarchy of legislation such that no legal rule of whatever nature may contradict the constitution. Consequently, any law or legislation infringing any article in the Constitution is deemed unconstitutional and inapplicable. Furthermore, "the constitution establishes a country's innate characteristics and sovereignty and outlines the rights and responsibilities of its citizens. Ideally, it guarantees basic human rights of the people, defines the system of governance, the legislative, executive and judicial branches (and their separation), and the obligations and duties of each element of government." (Clegg, M., 2016, p. 4).

The Jordanian constitution in force today is the one ratified by King Talal on January 1st, 1952 (the "**Constitution**"). Article 1 of the Constitution stipulates that Jordan is part of the Arab Nation and its ruling regime is parliamentary with a hereditary monarchy.

Article (1) of the Jordanian Constitution provides that: The Hashemite Kingdom of Jordan is an independent sovereign Arab State. It is indivisible and inalienable and no part of it may be ceded. The people of Jordan form a part of the Arab Nation, and its system of government is parliamentary with a hereditary monarchy. Jordan is considered as a monarchy, compared to Palestine, which applies a presidential system, article 5 provides that: The system of government in Palestine is a parliamentary democratic system based on political and party pluralism, in which the President of the National Authority is elected directly by the people and the government is accountable to the President and the Palestinian Legislative Council.

The Jordanian Constitution, in its third chapter, establishes and addresses three authorities:

1.1 **Legislative Authority:**

Pursuant to Article 25 of the Constitution (The corresponding Article of the Palestinian Basic Law is 47), the legislative authority shall be vested in the Parliament and the King. The Parliament shall consist of the House of Representatives elected by the

Jordanian people and the Senate appointed by the King. It should be noted that the number of senators must not exceed half the number of the deputies. The president of each of the House of Representatives and the Senate is elected by the deputies and the King respectively. The parliament has a term of four years and the requirements for eligibility of both the representatives and the senates have been listed in the constitution.

The duties of the legislative branch can be summarized in the following: (i) enacting laws: laws cannot be promulgated unless passed by both the Senate and the House of Representatives and ratified by the King; (ii) monitoring governmental actions through casting votes of confidence or no confidence in the Cabinet or any of the Ministers; and (iii) Questioning Ministers, through enquires and direct questions, and approving the state's public budget.

- **Cyberspace and the Legislative Authority:**

As presented earlier, the Legislative Authority is in charge of passing all the laws in the Jordanian legal system, hence, all legal rules that regulate cyberspace and the digital transactions in Jordan have to be approved by this Authority; the most important of which is the Jordanian Cybercrimes Law no. 27 for the year 2015 (The corresponding Palestinian law is the Law for Cybercrimes no. 16 for the year 2017), which will be addressed with more details in the following chapters. Other related laws are: the Jordanian Law of Communications no. 13 for the year 1995 and the Law for the Jordanian Electronic Transactions no. 15 for the year 2015.

1.2 **Executive Authority:**

Article 26 of the Constitution stipulates that the executive authority shall be vested in the King, and he shall exercise it through his ministers in accordance with the provisions of the Constitution (the corresponding articles in the Palestinian Basic Law are articles 38, 63, 64 & 65).

The Executive Authority is in charge of applying all the laws passed by the Legislative Authority, it also supervises such application; this is done in at different stages and phases. This Authority passes the Regulations and the Instructions and Decrees that puts the Laws into effect. At the same time, and as far as cybercrimes are concerned, the Public Prosecutor and the Unit for combating cybercrimes, are branches of this Authority.

- **Cyberspace and the Executive Authority**

Cyberspace is regulated by different rules at different stages; some of those rules are passed by the Executive Authority. Communications and digital transactions in general are greatly regulated and supervised by different governmental bodies at different levels. Cyberspace in both, private and public domains, is regulated, developed and administered by entities within this Authority.

Note: Many Regulations are passed by the Jordanian Cabinet, this also applies to Instructions and Governmental Strategies that regulate cyberspace in different aspects; some of which are: Instructions for publishing 'open government data' on the open data platform for the year 2019; the Government Policy Document in the Information, ICT and Post sectors for the year 2012; the General Policy for Inclusive Services in the Telecommunications Sector; the National Electronic Commerce Strategy; and the Strategy for Security and Information Protection.

1.3 **Judicial Authority:**

According to Article 27 (Articles 97 to 100 of the Palestinian Basic Law), the judicial authority shall be independent and exercised by the courts in their different types and levels. All judgments shall be issued in accordance with the law and in the name of the King.

The judicial authority's role is to settle any dispute that arises between the individuals themselves or between the individuals and the state by implementing the applicable legislations in Jordan (Articles 97-110 of the Jordanian Constitution and articles 97 to 100 along with article 31 of the Palestinian Basic Law).

Article 97of the Constitution (Articles 97 & 98 of the Palestinian Basic Law) stipulates that judges are independent and are subject to no authority other than that of the

Law. According to Article 98 (Articles 99 to 101 of the Palestinian Basic Law) judges of civil and religious (sharia) courts are appointed and dismissed by a Royal Decree in accordance with the provisions of the Law. The Constitution divides the courts of Law into three types: (i) Civil Courts which are ordinary courts of law that deal with civil and criminal cases; (ii) religious courts which are divided into Sharia courts and Tribunals of other religious communities acknowledged by the state; and (iii) special courts which include Municipal, Income Tax, Military, and Police Courts. According to the Constitution, courts of all types are open to all people and protected from any interference in their affairs (UN, DESA, 2004).

- **Cyberspace and the Judicial Authority**

As will be presented later, cyberspace is regulated in both civil and criminal laws; any dispute that takes place in cyberspace transactions can be settled at different Jordanian Courts. Cybercrimes are prosecuted at different Jordanian Criminal Courts, depending on the category of the criminal act.

It should be noted that the Jordanian constitution endorses the principle of the flexible separation between the authorities meaning that each branch is considered independent and is specialized in certain matters; however, cooperation between the branches is demanded to achieve and enact the strategies to administer the Kingdom.

1.4 **Fundamental rights and duties of Jordanians**

With regards to the basic rights included in the Constitution, the second chapter of the Constitution outlines such rights (Articles 9 to 33 of the Palestinian Basic Law). Firstly, Article 6/1 states that Jordanians shall be equal before the law with no discrimination between them in rights and duties even if they differ in race, language or religion. Furthermore, public freedom is a right guaranteed by the Constitution, especially freedoms of opinion and expression especially in respect of religious belief and the formation of political parties and associations. Furthermore, the Constitution ensures respect for the inviolability of private life and inviolability of the home and the right to education and employment. The Constitutions also grants the right of ownership whereby No property of any person shall be expropriated except for public utility and in consideration of a just compensation as shall be prescribed by law.

The above-mentioned articles outlines a few examples of the basic rights enlisted in the second chapter of the Jordanian constitution, being enlisted in the supreme law in the hierarchy no legislation below the constitution can violate any of the rights in the constitution, on the contrary the laws enacted in the Kingdom must further protect and broaden these rights (Alshdaifat, Sh., 2014, p. 31).

- **Cyberspace and Fundamental rights**

In cyberspace, the most relevant fundamental and constitutional rights and freedoms, that should be safeguarded, are: the freedom of expression or speech (Article 15 of the Jordanian Constitution &article 19 of the Palestinian Basic Law), freedom of information, the right to privacy and personal life (articles 7 & 18 of the Jordanian Constitution), articles 11 & 17 of the Palestinian Basic Law addresses the right to privacy, and article 27 addresses the freedom of press, there is no mention to the right to private communications as in the Jordanian Constitution.

Other relevant rights are ownership and property rights (Article 11 of the Jordanian constitution & article 21 of the Palestinian Basic Law), along with the freedom of communications (article 18 of the Jordanian Constitution)(Alkhatib, 2006).

Article 19/2 of the International Covenant on Civil and Political Rights include the freedom to receive and communicate information, ideas and opinions through the Internet. Article 19/3 provides that:

The exercise of the right provided in paragraph two of this article carries with it special duties and responsibilities. It may therefore be subjected to certain restrictions, but these shall only be such as are provided by law and are necessary:

*(**a**) For respect of the rights or reputations of others;*

*(**b**) For the protection of national security or of public order, or of public health and morals.*

2. **International Treaties and Conventions**

With regards to the international treaties and conventions, it must be noted that while the Jordanian legal system does not explicitly grant the international treaties and conventions a specific status among its hierarchy of legislation, the Jordanian Supreme Court, however, confirmed in many of its decisions that the international treaties and conventions fall directly under the constitution in the hierarchy of legislation and as such are superior to the laws, regulations and instructions.
The status of international treaties and conventions in the Palestinian legal system is not as clear, the courts have different stands on this issue (Twam, R., 2019).

- **Cyberspace and International Treaties**

Cyberspace is better regulated in an international setting, this is obviously due to the transnational nature thereof, therefore, many international treaties addressed cyberspace, especially cybercrimes; the most important of which are: The Council of Europe's Convention on Cybercrime, the Convention on Cybercrime (2001), also known as the Budapest Convention; The Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003); the Arab Convention for Combating Information Technology Crimes (2012) (all of which will be further addressed in chapter 4).

3. **Laws**

The laws passed by the legislative authority fall on the third level of the hierarchy of legislation in Jordan and the legislative branch is considered the authority having the general jurisdiction to issue laws. The laws issued by the legislative authority are what mainly govern our daily lives, interactions and conducts. These laws are divided into two categories which are public law and private law, which will be discussed in further detail below.
Laws are formal rules to govern behavior and transactions, protect individual rights and promote social policies; they are the mechanism by which states define the rules necessary to maintain social order and security, and to promote economic and social interests (Clegg, M., 2016, p. 8). Laws play an important role in balancing the above-mentioned rights and duties between citizens and between citizens of a state and the state itself. Laws constantly respond to sociology and the needs of a society, hence, they develop and adapt thereto, i.e. laws change over the time. Laws also give jurisdiction to those bodies responsible for law enforcement.

4. **Regulations (by-laws)**

The executive authority consists of the King who exercises his power through the prime minister and the ministers (the Cabinet). Article (45) of the Constitution granted the general authority in running the country to the cabinet; through applying and enacting the law and establishing a strategy to administer the country's affairs (article 45 of the Jordanian Constitution).
The Cabinet Ministers who are responsible for all state affairs, internal and external, execute the public and administrative duties. The Cabinet is authorized to set provisional Law in specific cases in the absence of Parliament. Moreover, the Executive Power is entrusted with setting regulations that are consistent with the provisions of the Law. The regulations issued by the executive authority fall on the fourth level of the hierarchy of law in Jordan, the regulations can under no circumstance infringe any of the principles listed in the laws issues and enacted by the legislative authority.

5. **Instructions and decrees**

Instructions are at the bottom of the hierarchy of legislation, therefore, they cannot contradict any other written legislation. Similar to regulations, instructions are passed by the Executive branch. Instructions and formal decrees are simple legal instruments that are flexible, in the sense that they can be easily amended, hence, most of the technical rules or guidelines are laid out using this legislative instrument.

List of additional material
Section 1
Number

Section Title **Introduction to Law and Legal Systems**

Content

Alkhatib, Noman Ahmad; Political Systems and Constitutional Law; first edition; Dar Althaqafa Publication and Distribution; 2006, Amman; Jordan
Alshdaifat, Shadi; Review of Human Rights under the Jordanian Constitution; Journal of Law; Policy and Globalization; ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online); Vol.29; 2014.
Clegg, Michael; Ellena, Katherine; Ennis, David; Vickery, Chad; The Hierarchy of Laws: Understanding and Implementing the Legal Frameworks that Govern Elections; International Foundation for Electoral Systems; 2016; file:///C:/Users/user/Documents/FORC/chapter/topic%201/SSRN-id3318872.pdf
Twam, Rashad; Khalil, Asem; the Enforcement of International Conventions in Palestine: Legal problems and constitutional solutions; Birzeit University; January 2019; Palestine.
UN, Department of Economic and Social Affairs (DESA); Hashemite Kingdom of Jordan Public Administration Country Profile; Division for Public Administration and Development Management (DPADM); February 2004.

Content

Section Number 1 (Introduction to Law and Legal Systems)

Section Title **Cyberspace and the law**

Introduction Law touches everything in our daily life, so does cyberspace; everything we do must be legal, and most of what we do is becoming digital, hence, the interrelation between cyberspace and the law is quite noticeable.
Cyberspace is regulated by many rules that fall in the hierarchy of legislation presented earlier, starting from the constitution and all the way down to the instructions; despite the fact that there is a limited number of legislation that specifically regulate cyberspace, it is, however, addressed by a large number of rules, in both, private and public domains, and by both civil and criminal laws, yet, mostly by the latter.
Law in general is divided into private law and public law; it is also divided into civil and criminal law, both divisions overlap, yet, each with a different approach.

Content 1. **Private Law vs. Public Law**
The law is divided into two sections, private and public law. The main difference between public law and private law lies in the fact that public law protects society as a whole and private law governs interactions between individuals or groups. Hence, public law is typically determined and enforced by government agencies, whereas private law addresses interactions within private (not public) persons. In public law the state acts with state authority.
Private law is the section of law that regulates private (not public) interactions between individuals (i.e. the state is not a party thereto), such as civil, commercial and labour laws. Private (or civil) laws also include family laws and rules that regulate civil status.
The Jordanian Civil Code is considered the general law which regulates the interactions between private individuals, their rights, duties, properties and relations, which do not directly concern the state. Commercial law regulates a special category of private interactions which involve merchants and their work and corporations (which are regulated also by the Law of Companies). Finally, labour law regulates the interactions between employers and their employees and work conditions.
Public law governs the interactions of the state with other parties, where the state is in a position of power. Of its branches, public international law, constitutional law, criminal law and administrative law. Public international law is the branch of law which governs the interactions of the state with other members of international law (such as states and international organizations); the constitutional law outlines the ruling regime and the basic rights as explained in detail above; finally the criminal law defines the acts that constitute a crime and the penalties thereto (which will be addressed with more details hereunder and in other chapters).

Cyberspace is regulated by both, private and public laws. In the private section, all laws are relevant, whether directly or indirectly; ownership of software and hardware, digital transactions (i.e. contracts), media, advertisements (adds), electronic commerce, intellectual property are some examples thereto. In the public sector, the most important law is the Jordanian Penal Code, which provides the general principles of crime and punishment in Jordan, however, digital crimes are specifically regulated by the Jordanian Cybercrimes Law no. 27 for the year 2015, as provided hereunder.

2. **Criminal Law vs. Civil Law**

Two of the most important laws in the public and private sections are the criminal law and the civil law respectively. Their importance lies in the fact that they are the two main sources of liability or responsibility: criminal and civil.

In a civil law setting, a person becomes legally bound or liable in many different manners, either voluntarily or involuntarily, such as contracts and torts. Civil law deals with behaviour that constitutes damage to an individual or other private party, such as a corporation. Examples are: breach of contract, negligence, and property damage.

Criminal law deals with behaviour that is or can be construed as an offense against the public, society, or the state, even if the immediate victim is an individual.

Criminal liability arises due to the violation of the penal code of a country, hence, such a code should be clearly written, and should provide explicitly criminalized acts and their punishment. Criminal liability is of extreme importance as it is concerned with depriving an individual from their freedom by imprisonment (sometimes forcing fines), which is considered an exception to the right of freedom provided by the constitution, hence care must be taken while organising crimes and sanctions.

Criminal law and civil law differ with respect to how cases are initiated (who may bring charges or file suit).

In criminal cases, for example, only the public prosecutor may initiate a case; punishment for serious (felony) charges often consists of imprisonment but may also include a fine paid to the government; to secure conviction, the prosecution must establish the guilt of the defendant "beyond a reasonable doubt".

In civil cases, by contrast, cases are initiated by a private party (the plaintiff), and are settled either in a court of law or via arbitration and similar private dispute-settlement methods; if the judge decides civil liability of any party, the effect almost always consists of a monetary award and never consists of imprisonment.

Cybercrimes law is considered part of the criminal law falling under public law, meaning that the state possess a position of power and sovereignty in any interaction governed by the cybercrimes law.

3. **Cyberspace in criminal law: cybercrimes**

A crime, by definition, is: "An action or omission which constitutes an offence and is punishable by law," crimes affect the public and their interests, they are acts against the society, and therefore, they can only be initiated – as presented earlier – by the public prosecutor.

The most important law addressing cyberspace is the Cybercrimes Law no 27 for the year 2015; however, all other laws are applicable. Crimes are divided into several categories according to the interest they are set out to protect, or to their severity (number of years of imprisonment).

Note: The second chapter of this book will explain the concept and elements of crime in general, and the categories of cybercrimes, in particular. The third chapter will address the digital evidence and the investigation thereto.

3.1 **Misdemeanours vs. Felonies**

Most legal systems divide their crimes into several different categories depending on the seriousness of the crime. The major categories are: infractions (minor violations), misdemeanors, and felonies. These categories are almost always determined by the maximum potential jail time that is possible for the crime.

In general, infractions are the least serious type of crime, they are usually punished with a fine. Misdemeanors, however, are more serious crimes, they can be punished by imprisonment up to but not exceeding three years, the punishment might also include a fine. Felonies, however, are the most serious crimes, hence, the

punishment for committing felonies can get to life imprisonment or capital punishment.

3.2 **Crimes against individuals vs. Crimes against property**

Usually, crimes in most criminal systems take this division, in the sense that crimes that affect humans (materially and morally) are usually more serious that crimes that affect property. This categorization is also applied to cybercrimes, however, the impact of digital age on societies and the widespread of cybercrimes necessitated a different approach or categorization to cyber-related acts or crimes. Therefore, criminal laws are changing to respond to the mall effect of digital age on the society. Consequently, cybercrimes are categorized into two categories: conventional cybercrimes and cybercrimes per se. This is to differentiate between conventional crimes that are committed via cyberspace and crimes against cyberspace. To illustrate, defamation is a conventional crimes, however it can be committed through cyberspace ,not only that, cyber-defamation is easier to commit and more widespread, hence, more damaging. On the other hand, hacking or illegal access to digital systems are crimes that could cause material or moral damages, but whether or not this damage took place, they are criminalized in most recent criminal laws; they are perceived as crimes against cyberspace .

Law is a social phenomenon that responds to societal needs, conventionally, penal laws address crime in response to its effect, thus, the categorization of crimes against individuals and property corresponds to this historical background. Cyberspace and cybercrimes are perceived as a modern phenomenon that demands corresponding measures, either by establishing new laws criminalizing malicious acts in cyberspace that are, evidently, not criminalized in conventional criminal laws, or by adopting a stricter approach to conventional crimes committed via cyberspace (ITU, 2012). Legislators worldwide are responding to immense interaction between cyberspace and crime, therefore, there is a tendency towards a stricter approach towards cybercrimes, whether committed using cyberspace or against cyberspace.

List of additional material

Section Number 1

Section Title **Introduction to Law and Legal Systems**

Content ITU, International Telecommunication Union; Understanding cybercrime: Phenomena, challenges and legal response; September 2012; Telecommunication Development Bureau; Place des Nations; CH-1211 Geneva 20; Switzerland; www.itu.int; http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CybcrimeE.pdf

Content

Section Number 1 (Introduction to Law and Legal Systems)

Section Title **Conclusion**

Content This chapter addressed the Jordanian legal system; in an attempt explain the structure of this system, the hierarchy of legislation, where the constitution sits on top of the legislative pyramid, then come the international conventions then laws, regulations and lastly instructions; and the implications of this pyramid, where rules on the bottom should not contradict any higher rules. The constitution, the supreme legislation in the legal system establishes the three main pillars of governance, the three powers or authorities: Legislative, Executive and Judicial; and how, on the one hand, these authorities furnish for and interact with for the rules regulating cyberspace; and, on the other hand, how the different tiers of legislation provide the legal infrastructure thereto. Arriving at cybercrimes and where they fit in the criminal legal system, between infractions, misdemeanors and felonies, and between crimes against individuals and/or property.

Content
Section Number 1 (Introduction to Law and Legal Systems)
Section Title **Table of contents**
Content **Foundation of the Legal System**

Hierarchy of Legislation
1. The constitution
1.1 Legislative Authority
- Cyberspace and the Legislative Authority
1.2 Executive Authority
- Cyberspace and the Executive Authority
1.3 Judicial Authority
- Cyberspace and the Judicial authority
1.4 Fundamental rights and duties of Jordanians
- Cyberspace and fundamental rights
2. International Treaties and Conventions
- Cyberspace and International Treaties
3. Laws
4. Regulations (by-laws)
5. Instructions and decrees

Cyberspace and the law
1. Private Law vs. Public Law
2. Criminal Law vs. Civil Law
3. Cyberspace in criminal law: cybercrimes
3.1 Misdemeanours vs. Felonies
3.2 Crimes against individuals vs. Crimes against property

Activity Number	1
Title	Identify the implications from the following video on the cybercrime laws.
Type	Reflection
Aim	Understand the main concepts related to cybercrimes (presented in sub-section: cyberspace and the law), it also serves as a preparation for the concepts in chapters 2 & 3.
Description	The following video presents a story about fishing, hacking and theft (by Glen Gooding); it explains, in a different perspective, the sub-section titled: Cyberspace and the law. It helps in identifying the role (and importance) of cyber-laws in regulating cyber-activities. https://www.youtube.com/watch?v=Cm3d0920Ohw
Timeline	Time: 1 hour
Assessment	Each student is required to submit a one-page report summarizing the following video with inference on the cybercrime laws.

Activity Number	2
Title	**Find cyber-rules**
Type	Research
Aim	Understand the main legal concepts and legal rules presented in sub-section: hierarchy of legislation.
Description	Conduct a search in different legislation and list the rules (articles) that you find more relevant to cyberspace, with clear reference to the legislation they follow, and rank them according to the legislative hierarchy
Timeline	Take home exam
Assessment	Each student is required to submit a one-page report of the list of rules

Think (MCQs)

Number 1

Title Subsection: Foundation of the legal system

Type Fill in the blanks

Question In the following paragraph, fill in the blanks that describe legal rules:
Legal rules are considered (i) ___ and (ii) ___ rules applying to all members of the community without any discrimination of whatever nature; (iii) ___ rules governing the conduct and behavior of individuals; and (iv) ___ rules accompanied by penalties and sanctions thus guaranteeing its proper implementation.

Answers (i) Abstract. (ii) General. (iii) Social. (iv) Obligatory.

Think (MCQs)

Number 2

Title Subsection Hierarchy of legislation

Type Rank options

Question Rank the following types of legislation according to the hierarchy of legislation in Jordan:

- Regulations
- Constitution
- Instructions and decrees
- International treaties and conventions
- Laws

Answers The Jordanian hierarchy of legislation is as follows:

1. Constitution;
2. International treaties and conventions;
3. Laws;
4. Regulations;
5. Instructions and decrees.

Think (MCQs)
Number 3
Title Subsection Hierarchy of legislation
Type Match pairs
Question

The legislative authority	Apply laws
The executive authority	Check the correct application of laws
The judicial authority	Issue laws

Answers
The legislative authority -------- Issue laws
The executive authority --------- Apply laws
The judicial authority --------- Check the correct application of laws

Think (MCQs)
Number 4
Title Subsection: Cyberspace and the law
Type Multiple choice question
Question The main difference between public law and private law is in:
Answers a. The issuing authority
b. **The rights they protect.**
c. All of the above.
d. None of the above.

Think (MCQs)

Number 5

Title Subsection: Cyberspace and the law

Type Rank options

Question Rank the following types of crimes according to their seriousness and their punishment, from bottom to top:
- Misdemeanors
- Infractions
- Felonies

Answers 1. Infractions.
2. Misdemeanors.
3. Felonies.

Extra

Number 1

Title **Jordan Country Profile**
Hashemite Kingdom of Jordan Public Administration Country Profile, Division for Public Administration and Development Management (DPADM) Department of Economic and Social Affairs (DESA) United Nations, February 2004. Last visited 17 February 2019.

Topic Sub-Section: Foundation of the Legal System

Type Online report.

Extra

Number 2

Title **Political Systems and Constitutional Law**
Alkhateeb, Noman Ahmad; Political Systems and Constitutional Law; first edition; Dar Althaqafa Publication and Distribution; 2006, Amman; Jordan.

Topic Sub-Section: Hierarchy of Legislation

Type Text book.

Extra

Number 3

Title **Understanding cybercrime: Phenomena**
ITU, Understanding cybercrime: Phenomena, challenges and legal response; September 2012; International Telecommunication Union; Telecommunication Development Bureau; Place des Nations; CH-1211 Geneva 20; Switzerland; www.itu.int; last visited January 2019. http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CybcrimeE.pdf

Topic Sub-Section: Cyberspace and the law

Type Online report.

2. Overview of Cybercrimes

<table>
<tr><td colspan="2">Scope</td></tr>
<tr><td>Number</td><td>2</td></tr>
<tr><td>Title</td><td>Overview of Cybercrimes</td></tr>
<tr><td>Introduction</td><td>This chapter will address the concept of a crime, explaining the elements of crimes in general, and the different categories of cybercrimes in particular.</td></tr>
<tr><td>Outcomes</td><td>The student will be able to understand the following:
- What constitutes a crime in the legal system?
- The different elements of a crime and how this applies to digital crimes.
- The different categories of digital crimes in national and international laws.
- How digital crimes are punished in applicable laws.</td></tr>
<tr><td>Topics</td><td>What Constitutes a Crime

The Elements of a Crime
1. The Legal element
2. The Material element
3. The Mental element

The Categories of cybercrimes
1. The categories of cybercrimes under the Jordanian cyber law
1.1 the First category of cybercrimes
1.2 the Second category of cybercrimes
1.3 the Third category of cybercrimes
1.4 the Fourth category of cybercrimes
1.5 the Fifth category of cybercrimes
1.6 the Sixth category of cybercrimes
1.7 the Seventh category of cybercrimes
2. Categories of cybercrimes under the Council of Europe’s Convention on Cybercrime
2.1 Offences against confidentiality, integrity and availability of computer data and systems
2.2 Computer-related offences
2.3 Content-related offences
2.4 Offences related to infringements of copyright and related rights

Conclusion</td></tr>
<tr><td>Study Guide</td><td>
<table>
<tr><td>Task</td><td>Time</td></tr>
<tr><td>Preparation (Introduction and On-line Planning):</td><td>1.5 hrs</td></tr>
<tr><td>Textbook Content:</td><td>4 hrs</td></tr>
<tr><td>Thinking (online discussion review questions)</td><td>1.5 hrs</td></tr>
<tr><td>Tutorial Work on Law and Legal Systems</td><td>1.5 hrs</td></tr>
<tr><td>Related Course Work</td><td>1.5 hrs</td></tr>
<tr><td>Total</td><td>10 hrs</td></tr>
</table>
Required external resources:

- Almanasah, Osama A. and Alzubi, Jalal M.; Crimes Relating to Information Electronic Systems and Technology: A Comparative Study; Third edition; Dar Al-Thaqafa for Publishing & Distributing 2017; Amman; Jordan.</td></tr>
</table>

	- Al-Nawaysa, Abdullah; Crimes of Information Technology: Explanation of the Substantive Provisions in the Cybercrimes Law; First Edition; Darwael for Publishing & Distributing; 2017; Amman; Jordan. - Al-Saeed, Kamel; Explanation of the General Provisions in the Penal Code: A Comparative Study; Third edition; Dar Al-Thaqafa for Publishing & Distributing; 2011; Amman; Jordan.

Content Chapter 2 Overview of Cybercrimes

Author **Muath Al-Zoubi,**
Assistant Professor of Criminal Law, School of Law, University of Jordan

Section Number 2 (Overview of Cybercrimes)

Section Title **What Constitutes a Crime**

Introduction This section will answer the question of what constitutes a crime. In this regard, it should be stressed that there is no consensus regarding the definition of crimes committed using technology. This lack of consensus is reflected in the range of terminology used to describe these crimes. However, the expression 'cybercrime' is the most common expression used in the literature (Clough, Jonathan, p. 9-10).Additionally, the UN adopts the expression 'cybercrime' in the Council of Europe's Convention on Cybercrime.Interestingly, cybercrimes have been described using different expressions. By way of illustration: 'computer crime', 'crime by computer', 'computer-related crime', 'high technology crime', 'internet crime', 'digital crime', 'virtual crime', or 'IT crime'. The rationality behind using such expressions is that they refer to crimes which are committed using technology (Clough, Jonathan, p. 9-10).

Content It is important to note that in order to answer the question of what constitutes a crime, it is imperative to clarify the definition of crime. In this regard, it is to be noted that the Jordanian Penal Code (the same Code is applicable in Palestine), which is considered the main legal instrument that stipulates crimes and the punishments due for committing these crimes, has no specific definition of the term 'crime'.However, the Code defines certain expressions, which might constitute – under certain circumstances – cybercrimes. For instance, the Jordanian Penal Code, defines the expression 'defamation' as 'the imputation of a certain matter to a person – even if it was done with doubt – which might negatively affect his/her honor, dignity and expose him/her to the hate and scorn of society regardless of whether such a matter is punishable by law or not' (article 188/1)Another example is where the Jordanian Penal Code defines the expression 'libel' as 'assaulting the dignity and honor of another person or his/her reputation – even if it was done with doubt – without accusing him/her with a specific matter' (article 188/2).

Consequently, as a result of the absence of a specific definition of the expression 'crime' in the Jordanian Penal Code, the Jordanian jurisprudence tries to address this issue through stating that the any definition of the concept 'crime' should have the following elements: the first element is the behavior, and whether such a behavior is positive or negative. To be more precise, positive behavior, in this context, means behaving in a way which is forbidden by law. In contrast, negative behavior, in this context, means refraining from behaving in a manner which is required by the law. The second element is that the behavior, whether it is positive or negative, should be illegal. The third element is that the illegal behavior should disrupt one of the basic interests of society. The fourth element is that the illegal behavior should result from criminal will. The fifth element is that the illegal behavior should be subjected to a penalty or a precautionary measure (Al-Saeed, K.; 2011; p. 39-40).

Consequently, it can be said that there is no unified definition of cybercrime that can be relied on to clarify what is meant by cybercrime. Indeed, the Jordanian Cybercrime Law does not explicitly define the expression 'cybercrime'. However, it defines a number of expressions that are relevant to cybercrime. First, this Law defines

'Information System' as follows: 'a set of programs and tools designed to create, send, receive, process, store, or manage data or information electronically' (article 2 of the Jordanian Cybercrime Law (No 27 of 2015); in the Palestinian Cybercrimes Law no. 16 for the year 2017, the definitions are presented in article 1; however, the latter law has a more thorough approach to the categories of cybercrimes).
Second, the concept 'Data' has been defined in the Jordanian Cybercrime Law as follows: 'figures, letters, symbols, shapes, sounds and images that have no significance on their own' (article 2 of the Jordanian law).Third, to describe the concept 'Information', the Law uses the following definition: 'data that has been processed and has significant meaning' (article 2).Fourth, the Jordanian Cybercrime Law defines the concept 'Internet' as 'a link between more than one information system to acquire and exchange data and information' (article 2).Fifth, the concept 'Website' has been defined in the Jordanian Cybercrime Law as follows: 'a place where information on the Internet is available through a specific address'(article 2).Sixth, to clarify the meaning of the concept 'Permission', this Law adopts the following definition: 'the authorization granted by the person concerned or the competent judicial authority to one or more persons or the public to access or use an information system or the Internet in order to view, cancel, delete, add, change, re-disseminate data or information, block access, or stop the operation of the hardware, change a website or cancel or modify its contents'(article 2).Seventh, the Jordanian Cybercrime Law defines the expression 'Software' as follows: 'a set of orders and technical instructions intended to accomplish a task that can be implemented using information systems' (article 2).

List of additional material

Section Number	**2 (Overview of Cybercrimes)**
Section Title	**What Constitutes a Crime**
Content	Al-Saeed,Kamel; *Explanation of the General Provisions in the Penal Code: A Comparative Study;* third edition; Dar Al-Thaqafa for Publishing & Distributing; 2011; Amman; Jordan. Clough, Jonathan; Principles of Cybercrime; Cambridge University Press; 2015

Content	
Section Number	**2 (Overview of Cybercrimes)**
Section Title	**The Elements of the Crime**
Introduction	In general, there are three main elements of any crime. The first is the legal element; the second is the material element; and the third is the mental element.

Content

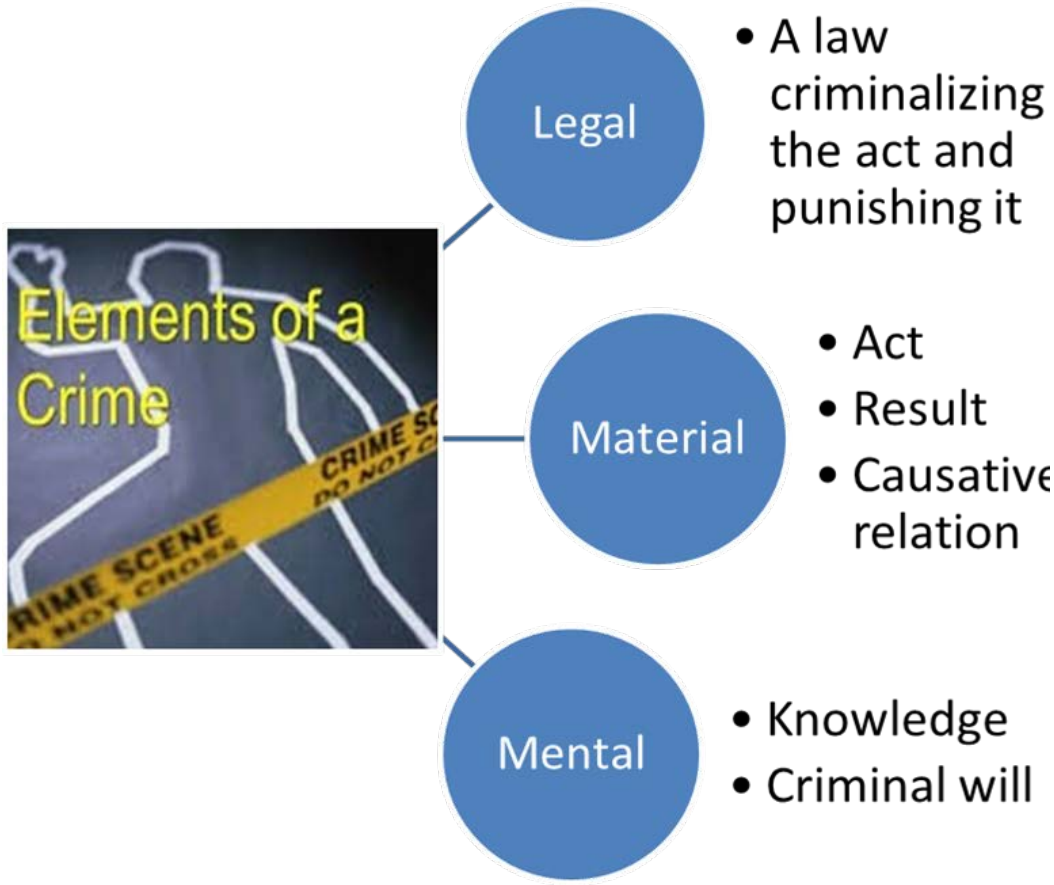


Figure (1) Elements of a crime

1. **TheLegal Element**

This element has been affirmed in the Jordanian Penal Code (Al-Zoubi, M.; 2015; p. 70).The Jordanian Penal Code has explicitly stated that 'there is no crime without legal stipulation and there is no penalty or measure that shall be imposed unless provided for by the law at the time the crime is committed' (article 3 of the Jordanian Penal Code).Likewise, the Jordanian Constitution affirms the principle of legality when it states that 'no person may be arrested, detained, imprisoned, have his/her freedom restricted, or be prevented from free movement except in accordance with the provisions of the law' (article 8/1 of the Jordanian Constitution).

This legal element could be referred to as the principle of legality; '*nullumcrimen, nullapoena sine lege*' (Hall, J.; 2005; p. 27-69).It is important to note that the principle of legality requires the existence of written rules in order to establish criminal offences. Therefore, if there is no provision for punishing the case before the judge, the judge should not establish a criminal offence for such a case. Consequently, in light of the above, sources of criminal legislation should not include custom and habit in order to establish crimes or to impose punishments (Al-Saeed, K.; 2011; p.56).

Furthermore, in accordance with the principle of legality, no one shall be prosecuted for committing an act before the issuance of a provision criminalizing such an act; in addition, no one shall be prosecuted for committing an act after the provision which criminalizes such an act is cancelled. Moreover, according to this principle, it is not permissible to apply the same rules for acts which have not been criminalized as for acts which have been criminalized, even if they are both similar with regard to motives, effectiveness, results or elements; as doing so would contradict the principle of legality. Additionally, it is not permissible to expand the principle of legality in the interpretation of provisions related to criminal matters (Almanasah, O.; 2017; p. 45).

2. **The Material Element**

The material element is an external action which has a physical nature. In this regard, it can be said that all crimes require the existence of a material element. It is noteworthy

that the material element is represented by the physical actions that constitute aggression against interests covered by criminal protection (Al-Majali, N.; 2015; p. 251).The material element includes three components. The first component is committing an act which is considered prohibited or refraining from acting when a person is legally obliged to act. This component is known as the *actus reus*. It also involves actual physical or verbal acts. Interestingly, the prosecutor is required to show the existence of the *actus reus* in order to establish a criminal case against the person in question. Notably, under this component, it is not only committing a prohibited act that brings a criminal liability but also the failure to act, or omission. However, this failure to act requires a legal duty in which such a duty is created by relationship, continuance of care obligation, statute or contract(Pollock, J.; 2015; p. 213).

The second component of the material element is the criminal result. To be specific, the criminal result is the effect of the criminal behaviorwhich has legal consequences (Almanasah, O.; 2017; p. 55).Interestingly, the component of the criminal result can be approached in two ways. The first approach is the physical approach. This approach is concerned with the external change that occurs as a result of the criminal behavior. By way of illustration, in the crime of theft, the money stolen moves from the possession of the victim to the possession of the offender. The second approach is the legal approach. This approach is represented by the violation of the interest that is protected by the law. For instance, in the crime of theft, the criminal result is a violation of the right to property, which is an interest that is protected by law (Al-Majali, N.; 2015; p. 258-259).

The third component of the material element is the causative relationship between the *actus reus* and the criminal result. What is evident is that the causative relationship has great importance in all crimes that require the component of the criminal result. It is noticeable that the causative relationship assigns the criminal result to the *actus reus*. Therefore, the causative relationship contributes towards identifying the scope of criminal liability in cases where there is a causative connection between the criminal result and the *actus reus*. Along with this, in case of the absence of a causative relationship between the *actus reus* and the criminal result, it is necessary to distinguish between two types of crimes. The first category is intended crimes; in this case, the absence of a causative relationship will result in the responsibility of the perpetrator being limited to an attempt to commit a crime. This is in contrast with the second category, which is the unintended crimes; in this case, the absence of a causative relationship will result in the absence of criminal liability. This is because there was no attempt to commit the unintended crimes (Al-Majali, N.; 2015; p. 260-261).

3. **The Mental Element**

The mental element is known as the *mens rea*. It is to be noted that this element is referred to as a criminal state of mind (Pollock, J.; 2015;2.13).Interestingly, the Jordanian Penal Code addresses the mental element through dealing with a number of issues. The first issue is intent, which the Jordanian Penal Code defines as follows: 'the will to commit the crime as defined by law' (article 63 of the Jordanian Penal Code).The Jordanian Penal Code further clarifies when a crime is to be regarded as a deliberate crime. In view of this, it asserts that 'a crime is considered to be a deliberate one even if the criminal consequence of the act exceeded the intent of the perpetrator, provided that the perpetrator expected such a consequence and accepted the risk of its occurrence'(article 64).The third issue is addressed when the Jordanian Penal Code highlights the issue of the motive for commission a crime, defining the motive as 'the reason which makes the perpetrator commit the act. Or, it is the ultimate result the perpetrator intends to achieve. A motive is not an incriminating element except in instances stipulated by the law'(article 67).The fourth issue is considered when the Jordanian Penal Code addresses the liability of persons. It requires the act to be committed consciously and willfully in order for the perpetrator to be sentenced for committing such an act. The Jordanian Penal Code explicitly states that 'no person shall be sentenced unless this person commits the act consciously and willfully' (article 74/1).

It is worth noting that the mental element has two components. The first component is knowledge. Knowledge here refers to knowledge of the elements of the crime. Such

knowledge is presumed as ignorance of the law does not consider (Almanasah, O.; 2017; p. 60-61).In view of this, the Jordanian Penal Code affirms that 'ignorance of the law shall not be an excuse for any person who commits a crime' (article 85 of the Code).To return to an earlier point, knowledge as a component of the crime involves the following factors: the first factor is knowledge of the facts which are considered components of the crime. The second factor is knowledge of the subject of the crime. The third factor is knowledge of the essence of the prohibited act or the failure to act and its danger(Almanasah, O.; 2017; p. 61).
The second component of the mental element is criminal will. Criminal will means psychological activity which aim to achieve a specific goal. It is noteworthy that criminal will has two aspects to it. The first is the criminal will of the *actus reus*. In order to bring criminal liability for an intended crime, prosecutors are required to prove that the perpetrator's criminal will was directed towards committing a prohibited act which endangered a right protected by the law. Furthermore, the first part of criminal will assumes that the perpetrator knows the gravity of his/her act in terms of the right protected by law and nonetheless commits the prohibited act or refrains from acting in a way that is required by law. The second aspect is the criminal will of the criminal result. This part is required for the completion of the mental element (Almanasah, O.; 2017; p. 62-63).

List of additional material

Section Number	2 (Overview of Cybercrimes)
Section Title	**The Elements of the Crime**
content	**Laws and Conventions:** The Council of Europe's Convention on Cybercrime, European Treaty Series - No. 185, Published 2001. The Jordanian Constitution (1952) page 3 of the Official Gazette (No 1093) dated 8 January 1952. The Jordanian Cybercrime Law (No 27 of 2015) page 5631 of the Official Gazette (No 5343) dated 1 June 2015. The Jordanian Penal Code, as amended (No 16 of 1960) page 374 of the Official Gazette (No 1487) dated 11 May 1960.
Content	**References:** Al-Majali,Nitham T.;*Explanation of Criminal Law General Section: Analytical Study in General Theory for Crime and Penal Liability;* Fifth edition; Dar Al-Thaqafa for Publishing & Distributing; 2015; Amman; Jordan. Almanasah, Osama A. andAlzubi, Jalal M.;*Crimes Relating to Information Electronic Systems and Technology: A Comparative Study;* Third edition; Dar Al-Thaqafa for Publishing & Distributing 2017; Amman; Jordan. Al-Saeed,Kamel; *Explanation of the General Provisions in the Penal Code: A Comparative Study;*Third edition; Dar Al-Thaqafa for Publishing & Distributing; 2011; Amman; Jordan. Al-Zoubi, Muath; 'An Analysis of the Crime of Trafficking in Persons under International Law with a Special Focus on Jordanian Legislation;' PhD thesis; Brunel University;2015; London. Hall, Jerome; *General Principles of Criminal Law;*The Lawbook Exchange, Ltd.; 2005. Pollock,Joycelyn M.;*Criminal Law;*Routledge; 2015.
Content Section Number	**2 (Overview of Cybercrimes)**
Section Title	**The Categories of Cybercrimes**
Introduction	This section will address two categories of cybercrimes. The first category is cybercrimes under the Jordanian Cybercrime Law. The second category is cybercrimes under the Council of Europe's Convention on Cybercrime.

Content 1. **Categories of cybercrimes under the Jordanian Cybercrime Law**

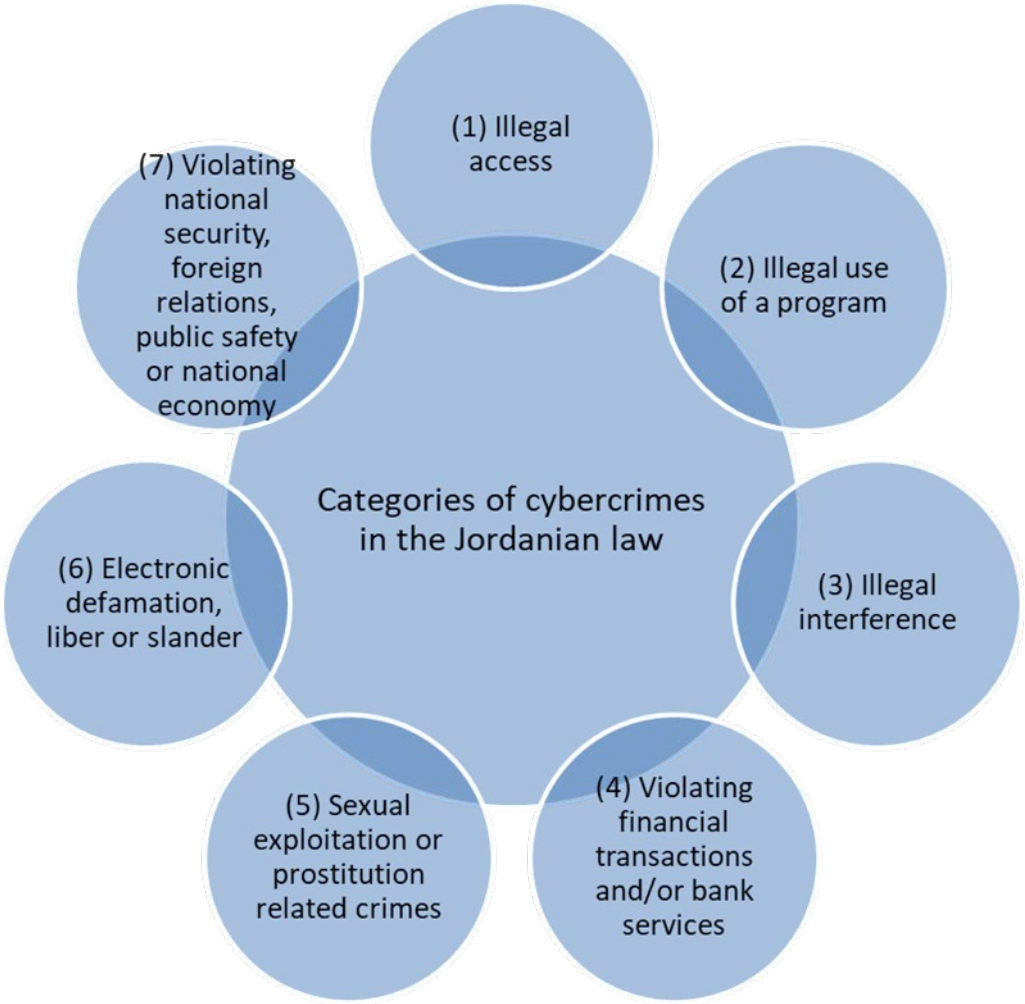


Figure (2): Categories of cybercrimes in the Jordanian Law

A number of cybercrimes have been stipulated under the Jordanian Cybercrime Law. These crimes are the following:

1.1 **The First Category of Cybercrimes (Illegal access)**

Figure (3): Illegal access

The first crime stipulated under the Jordanian Cybercrime Law is illegal access to the internet or any information system. This crime includes the following illegal practices. The first illegal practice involves 'intentionally accessing the internet or information system in any manner without authorization or in violation or excess of an authorization' (article 3/A of the Jordanian Cybercrime Law, and article 4 of the Palestinian Law).The second illegal practice comprises 'intentionally accessing the internet or information system for the purpose of cancelling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information or stopping or disabling the operation of the Internet or an information system of the Internet' (article 3/B of the Jordanian law).The third illegal practice involves 'intentionally accessing a website for the purpose of changing a website or cancelling, destroying or altering its content or assuming its identity or the identity of its owner' (article 3/C of the Jordanian law).

It is noticeable that the crime of illegal access to the internet or any information system is the first act to be criminalized under the Jordanian Cybercrime Law. This crime is similar to any crime with regard to the elements required; it requires the existence of the legal element, the material element and the mental element. Particularly, the legal element can be found in the legal provision criminalizing the act and imposing the punishment for committing such an act. In the crime of illegal access to the internet or any information system, the legal element is Article 3 of the Jordanian Cybercrime Law (article 3).The material element in this crime is represented by unauthorized access, which is considered to be the *actus reus*. In this regard, it should be stressed that access to the information system is not a crime *per se*unless it is done without authorization (Al-Nawaysa, A.; 2017; p. 213-219).Finally, the mental element in the crime of illegal access to the internet or any information system requires that this crime be committed intentionally. Therefore, the two main components of the mental element, which are knowledge and criminal will, are satisfied by this requirement (Al-Nawaysa, A.; 2017; p. 226).

The punishments for committing the crime of the illegal access to the internet or any information system under the Jordanian Cybercrime Law vary according to which illegal practice is committed. In particular, punishments for the first illegal practice are imprisonment (one week to three months), or a fine between 100 and 200 Jordanian Dinars, or both punishments. Additionally, the punishments for the second and third illegal practices are imprisonment (three months to one year) and by a fine between 200 and 1000 Jordanian Dinars (article 3 of the law).

1.2 **The Second Category of Cybercrimes (illegally use of a program)**

Figure (4): Illegal use of a program

The second crime stipulated under the Jordanian Cybercrime Law is the crime of illegally using a program in order to achieve an illegitimate purpose. This crime requires'intentionally installing,publishing or using a program through the internet or using an information system, with the purpose of cancelling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring, copying, capturing, or enabling others to view data or information, or obstructing, interfering, hindering, stopping the operation of an information system or preventing access to it, or altering a website or cancelling it, destroying it, or altering its content or operating it, assuming its identity or the identity of the owner without authorization or in excess of or in contravention of such an authorization' (article 4).

This crime has the following elements. The first element is the legal element, which is covered in Article 4 of the Jordanian Cybercrime Law (article 4).The second element is the material element, which includes the following components: installing, publishing or intentionally using a program. To be more precise, the installing component means adding programs by using the internet or information system. The publishing component means distributing programs by any means using the internet or information system. The using component means utilizing data or a program (Al-Nawaysa, A.; 2017; p. 260-261).The third element is the mental element: Jordanian Cybercrime Law implicitly states that this crime is required to be committed intentionally, which means that the perpetrator of this crime knows that he/she is committing this crime, as well as that he/she has the criminal will to commit such a crime (Al-Nawaysa, A.; 2017; p. 264).

What is evident in Article 4 is that the commission of the crime of illegal using of a program in order to achieve an illegitimate purpose is punishable by imprisonment (three months to one year) and a fine between 200 and 1000 Jordanian Dinars.

1.3 **The Third Category of Cybercrimes (Illegal interference)**

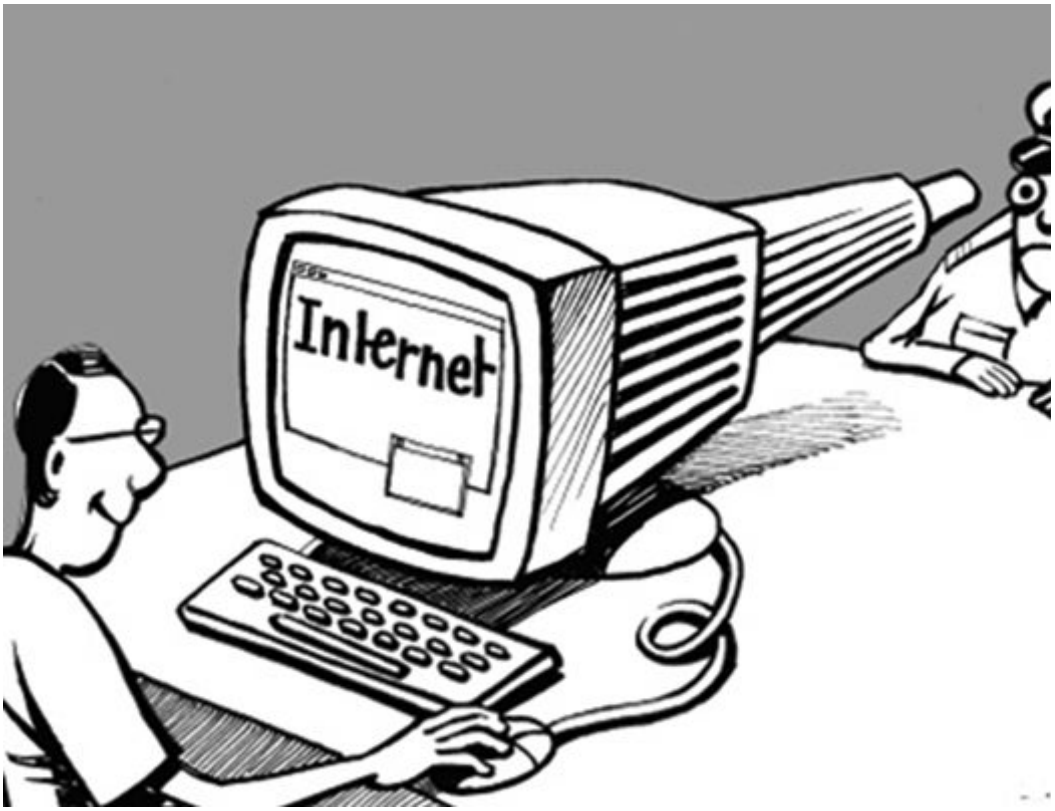


Figure (5): Illegal interference

The third crime stipulated under the Jordanian Cybercrime Law is the crime of interfering with what is transmitted through the internet or any information system. This crime requires 'intentionally capturing, interfering, intercepting, obstructing, altering or deleting what is transmitted through the internet or any information system'. This crime has three elements. Firstly, Article 5 of the Jordanian Cybercrime Law criminalizes this crime and imposes punishments for the commission of such a crime. This represents the legal element.Secondly, the necessary material element is stipulated in Article 5. Thirdly, the mental element is addressed implicitly, when Article 5 requires that this crime be committed intentionally. Consequently, if all three elements are met, the commission of this crime will result in imprisonment (three months to one year) and a fine between 200 and 1000 Jordanian Dinars.

1.4 **The Fourth Category of Cybercrimes (Violating financial transactions and/or bank services)**

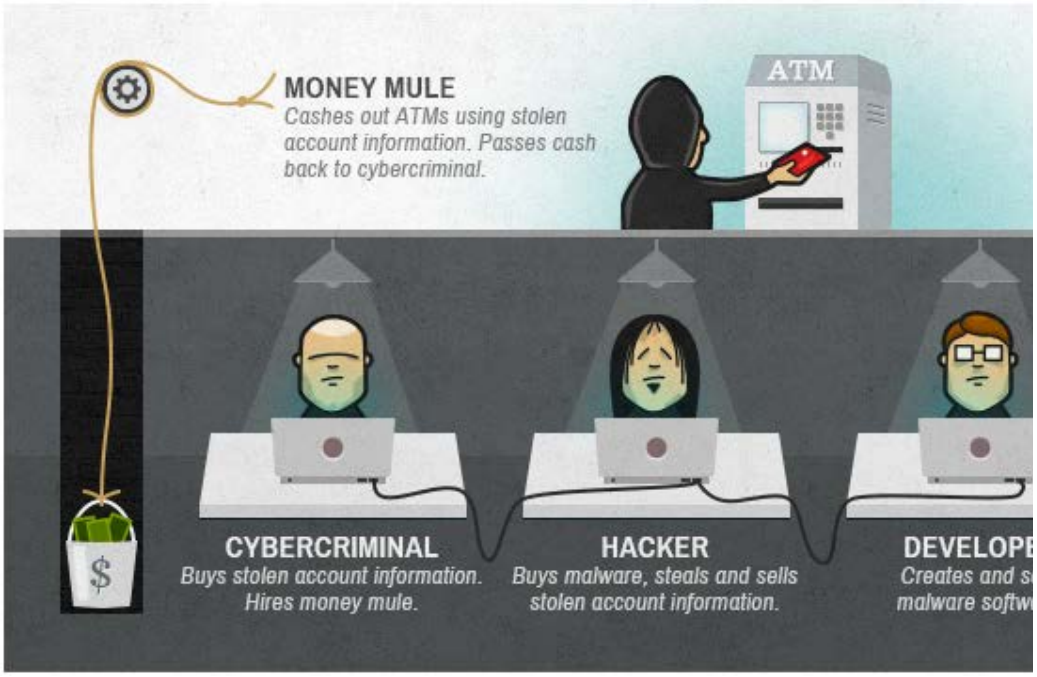


Figure (6): Violating financial transactions and/or bank services

The fourth crime stipulated under the Jordanian Cybercrime Law is the crime of violating financial transactions or banking services. This crime includes the following illegal practices: 'intentionally and without authorization obtaining through the internet or any information system data or information relating to credit cards or data or information that is used in the execution of electronic financial or banking transactions'(article 6 of the law);and 'committing any of the previous acts against any information system, website, or the internet relating to money transfer, payment services, clearing, settlements, or any banking services provided by banks and financial companies' (article 7).This crime has three elements, the first of which is the legal element. This element is illustrated in the two Articles criminalizing this crime. These are Articles 6 and 7 of the Jordanian Cybercrime Law.The second element is the material element. This element can be constituted by criminally obtaining data or information concerning credit cards, financial transactions or banking services (Al-Nawaysa, A.; 2017; p. 284-286).The third element is the mental element. In this regard, it should be stressed that this crime is required to be committed intentionally; consequently, the perpetrator should know the reality of his/her behavior and the elements of the crime. Additionally, the perpetrator should have the will to commit the act and the will to achieve the criminal result. It is noteworthy that the motive behind committing this crime is irrelevant(Al-Nawaysa, A.; 2017; p. 284-286).

The punishments for committing the crime of violating financial transactions or banking services differ according to which illegal practice is committed. More specifically, the punishments for the first illegal practice are imprisonment (one year to three years) and a fine between 500 and 2000 Jordanian Dinars (article 6 of the law).The punishments for the second illegal practice are imprisonment for a term not less than five years and a fine between 5000 and 15,000 Jordanian Dinars (article 7).

1.5 **The Fifth Category of Cybercrimes (Sexual exploitation or prostitution related crimes)**

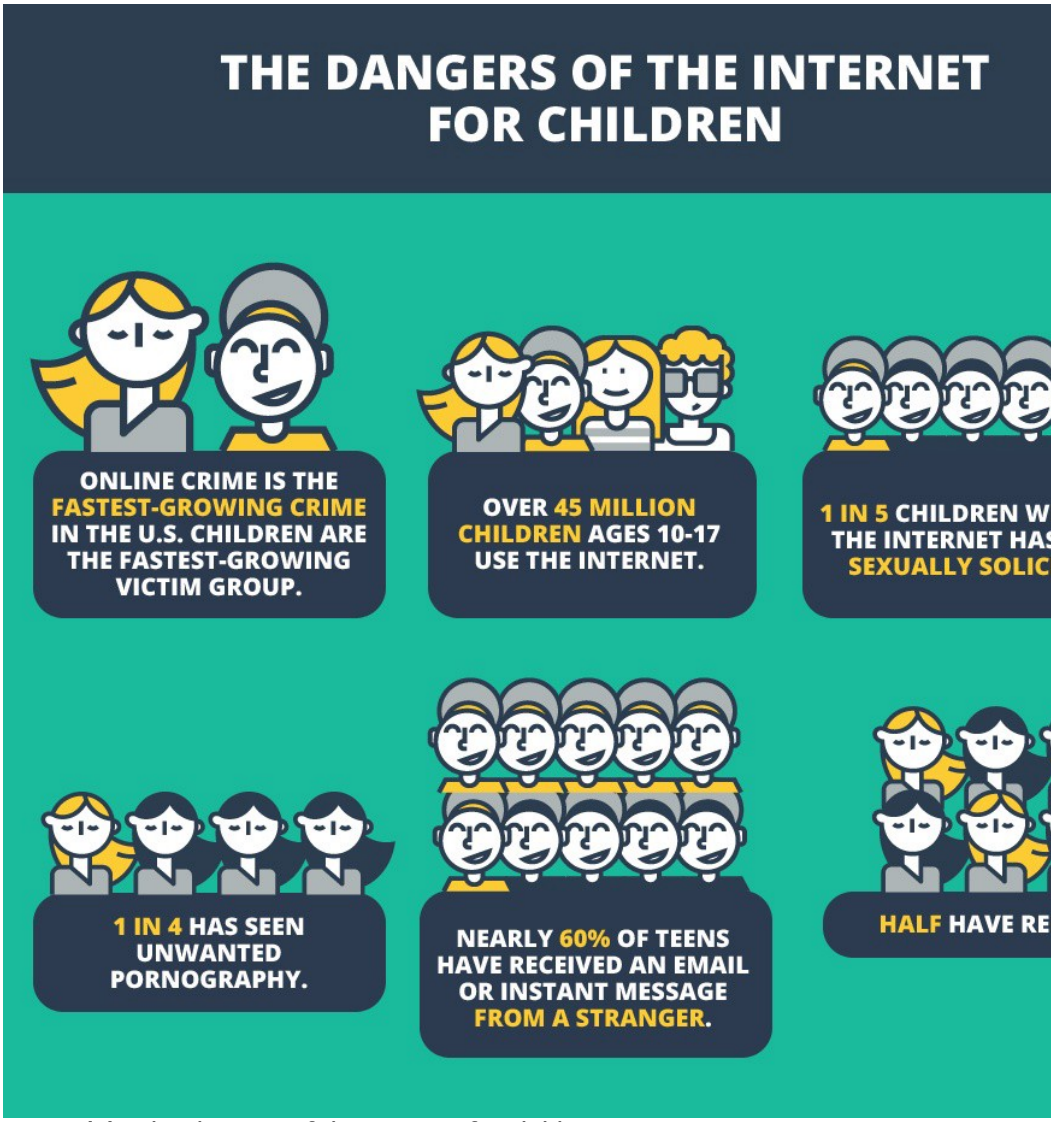


Figure (7): The dangers of the internet for children
Source: https://pixelprivacy.com/resources/keep-children-safe-online/

The fifth crime stipulated under the Jordanian Cybercrime Law is the crime of sexual exploitation or prostitution-related crimes. This crime includes the following illegal practices. The first is 'intentionally transmitting or publishing through an information system or the internet anything heard, read or graphic containing pornographic materials involving or relating to the sexual exploitation of those who have not attained eighteen years of age' (article 9/A).The second illegal practice is 'intentionally using an information system or the internet to create, prepare, store, process, display, print, publish or promote pornographic activities or work for the purpose of influencing those who have not attained eighteen years of age or those who are psychologically or mentally disabled, or direct or incite such persons to commit a crime'(article 9/B).The third illegal practice constitutes 'intentionally using an information system or the internet for the purpose of exploiting those who have not attained eighteen years of age or those who are psychologically or mentally disabled for prostitution or pornographic activities' (article 9/C).The fourth illegal practice is 'intentionally using the internet or an information system to create a website to facilitate or promote prostitution' (article 10). It is worth noting that the legal element of this crime can be found in Articles 9 and 10 of the Jordanian Cybercrime Law. Furthermore, the material element varies from one illegal practice to another. However, the material element in this crime should consist of the *actus reus*, the criminal result and the causative relationship between the *actus reus*and the criminal result. Additionally, the mental element requires the existence of knowledge of the elements of the crime as well as criminal will.

What is certain, however, is that the illegal practices consisting of the crime of sexual exploitation or prostitution-related crimes are punishable as follow: Firstly, punishments for the first illegal practice are imprisonment (three months to one year) and a fine between 300 and 5000 Jordanian Dinars (article 9/A).Secondly, punishments for the second illegal practice are imprisonment for a term not less than two years and a fine between 1000 and 5000 Jordanian Dinars (article 9/B).Thirdly, punishments for the third illegal practice are imprisonment by temporary servitude and a fine between 5000 and 15,000 Jordanian Dinars (article 9/C).Fourthly, punishments for the fourth illegal practice could be imprisonment for a term not less than six months and a fine between 300 and 5000 Jordanian Dinars (article 10).

1.6 **The Sixth Category of Cybercrimes (Electronic defamation, liber or slander)**

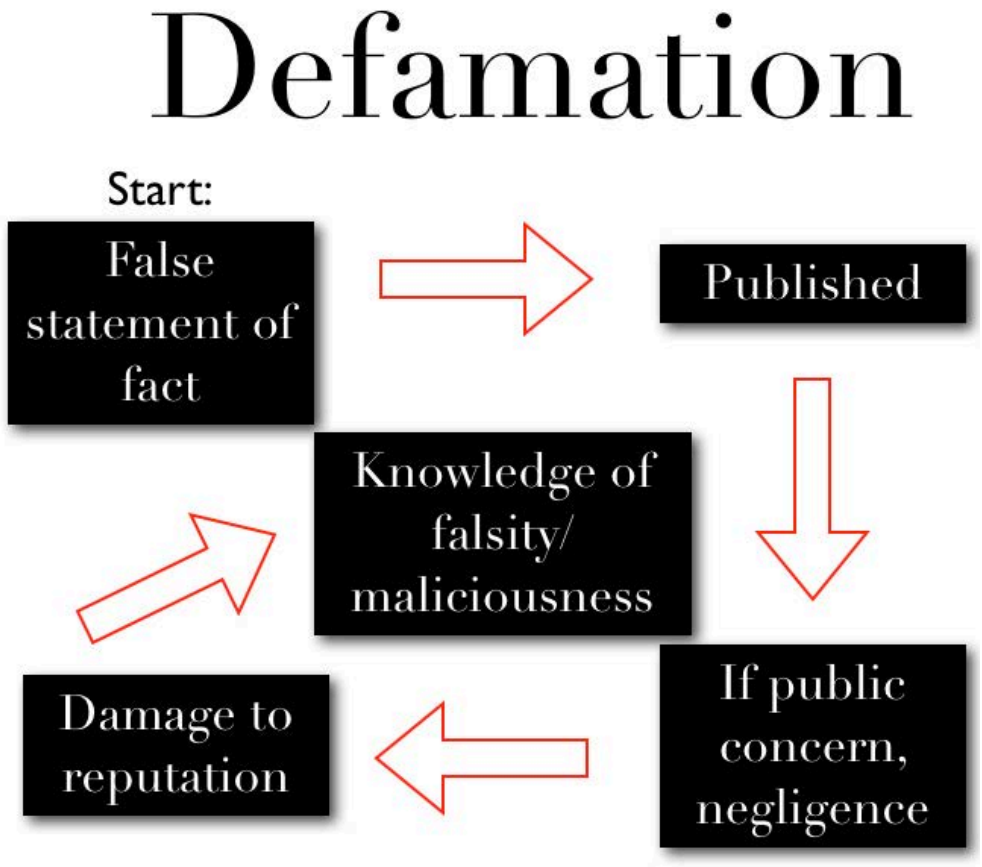


Figure (8): Defamation Process
Source: http://nikssinghal12345.blogspot.com/2014/01/cyber-defamation.html

The sixth crime stipulated under the Jordanian Cybercrime Law is the crime of electronic defamation, libel or slander. This crime requires 'intentionally sending, resending or publishing data or information through the internet, a website or any information system content of defamation, libel or slander'.This crime includes the following elements: the first is the legal element which appears in Article 11 of Jordanian Cybercrime Law.Secondly, the material element in this crime can be constituted by the *actus reus,* which includes sending, resending or publishing data or information. Thirdly, the mental element can be found in the existence of knowledge and criminal will. Specifically, the perpetrator should know the nature of his/her behavior. Therefore, the perpetrator should know that he/she is committing a criminal behaviorby sending, resending or publishing data or information. Additionally, the perpetrator should know that he/she is dealing with an electronic means. Moreover, the perpetrator should know that the data or information sent includes something which harms the victim. Along with this, the perpetrator should have criminal will. Consequently, the perpetrator should not

be forced to commit the criminal act (Al-Nawaysa, A.; 2017; p. 352-355).In light of the above, it should be stressed that the commission of this crime is punishable by imprisonment for a term not less than three months and by a fine between 100 and 2000 Jordanian Dinars (article 11).

1.1 **The Seventh Category of Cybercrimes (Violating national security, foreign relations, public safety or national economy)**

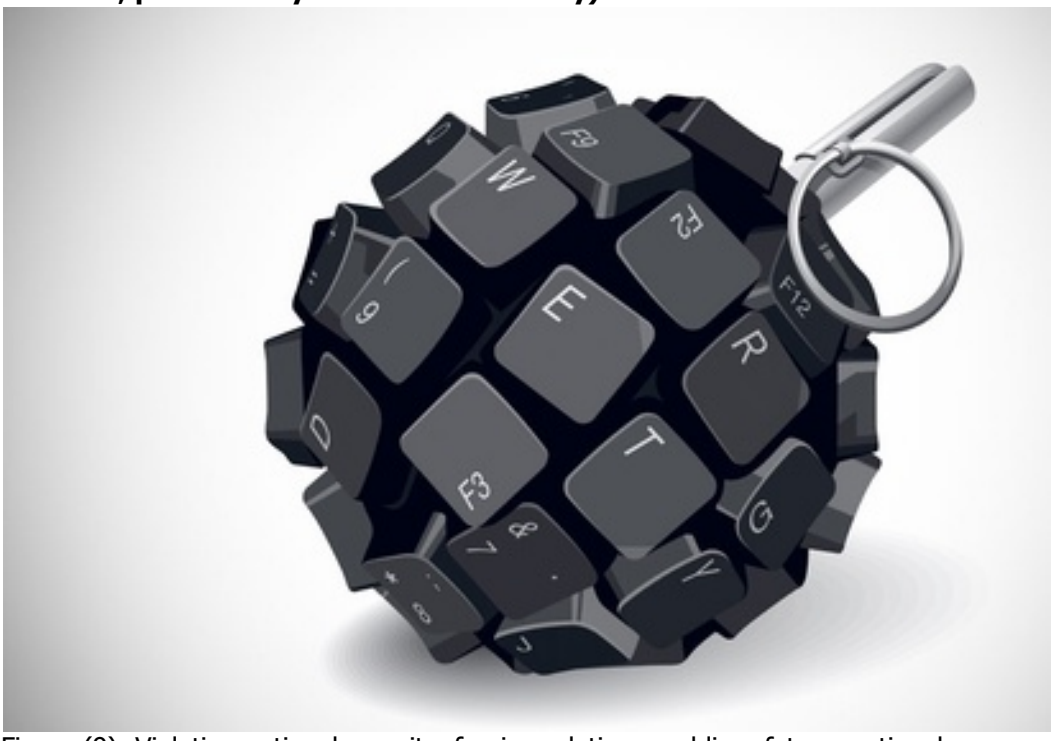


Figure (9): Violating national security, foreign relations, public safety or national economy

The seventh crime stipulated under the Jordanian Cybercrime Law is the crime of violating the national security, foreign relations, public safety or national economy of the Kingdom. This crime includes the following illegal practices. The first is 'intentionally and without authorization or in violation or excess of an authorization accessing the internet or information system in any manner with the purpose of viewing data or information that is not available to the public and which touches upon national security, foreign relations of the Kingdom, public safety or national economy' (article 12/A).The second illegal practice is 'intentionally and without authorization or in violation or excess of an authorization accessing the internet or information system in any manner with the purpose of deleting data or information, extinguishing, destroying, altering, changing, transferring, copying or disclosing data or information' (article 12/B).The third illegal practice is 'intentionally accessing a website with the purpose of viewing data or information that is not available to the public and which touches upon national security, foreign relations of the Kingdom, public safety or national economy' (article 12/C). The fourth illegal practice is 'intentionally accessing a website with the purpose of viewing data or information that is not available to the public and which touches upon national security, foreign relations of the Kingdom, public safety or national economy with the purpose of deleting, extinguishing, destroying, altering, changing, transferring or copying data or information' (article 12/D).

This crime requires three elements. The first is the legal element, and can be found in Article 12 of the Jordanian Cybercrime Law (article 12).The second element is the material element, which is represented by accessing, including accessing the internet or an information system without authorization or in violation or excess of an authorization. The third element is the mental element, which includes general *mens rea*and a special *mens rea*. The general *mens rea* has two components. The first component is knowledge and the second is criminal will. The special *mens rea* requires that the purpose of viewing data or information is to touch upon national security, foreign

relations of the Kingdom, public safety or national economy (Al-Nawaysa, A.; 2017; p. 378-379).
It is noteworthy that the punishments for committing the crime of violating the national security, foreign relations, public safety or national economy of the
Kingdom vary depending on which illegal practice is committed. To be more precise, the punishments for the first illegal practice are imprisonment for a term not less than four months and a fine between 500 and 5000 Jordanian Dinars (article 12/A). The punishments for the second illegal practice are temporary servitude and a fine between 1000 and 5000 Jordanian Dinars (article 12/B). The punishments for the third illegal practice are imprisonment for a term not less than four months and a fine of not less than 500 Jordanian Dinars (article 12/C). The punishments for the fourth illegal practice are temporary servitude and a fine between 1000 and 5000 Jordanian Dinars (article 12/D).

2. **Categories of Cybercrimes under the Council of Europe's Convention on Cybercrime**

Cybercrimes under the Council of Europe's Convention on Cybercrime are categorized in a different manner from the categorization applied by internal laws. Accordingly, cybercrimes are divided into four categories, as follows:

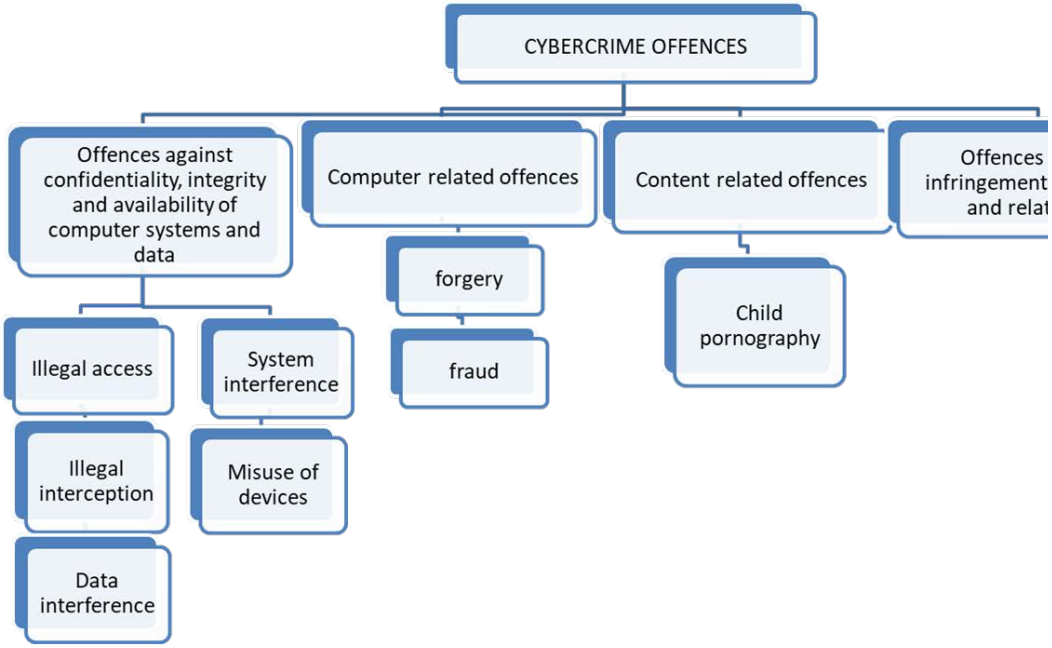


Figure (10): Categories of cybercrimes in Budapest Convention

2.1 **Offences against confidentiality, integrity and availability of computer data and systems**:

The first category of cybercrimes under the Council of Europe's Convention on Cybercrime is 'offences against the confidentiality, integrity and availability of computer data and systems' (section1, title 1). It is noteworthy that under the Council of Europe's Convention on Cybercrime, computer data has been defined as 'any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function' (article 1/B of the Convention).In addition to this, the Council of Europe's Convention on Cybercrimedefines a computer system as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data' (article 1/A).The following criminal offences constitute cybercrime. The first criminal offence is illegal access(article 2),the second is illegal interception (article 3),and the third is data interference (article 4).The fourth criminal offence is system interference (article 5),and the fifth is misuse of devices (article 6).

2.2 **Computer-related offences**

The second category of cybercrimes under the Council of Europe's Convention on Cybercrime is 'computer-related offences' (section 1, title 2).It is to be noted that under

the category of computer-related offences, there are two types of criminal offences. The first criminal offence is computer-related forgery (article 7). The second criminal offence is computer-related fraud (article 8).

2.3 **Content-related offences:**

The third category of cybercrimes under the Council of Europe's Convention on Cybercrime is 'content-related offences' (Section 1, title 3). What is evident is that content-related offences include child pornography relatedoffences (article 9).Under child pornography related offences, there are a number of conducts that are specifically criminalized. The first criminalized conduct is 'producing child pornography for the purpose of its distribution through a computer system' (article 9/a). The second criminalized conduct is 'offering or making available child pornography through a computer system'(article9/b).The third criminalized conduct is 'distributing or transmitting child pornography through a computer system' (article 9/c).The fourth criminalized conduct is 'procuring child pornography through a computer system for oneself or for another person' (article 9/d).The fifth criminalized conduct is 'possessing child pornography in a computer system or on a computer-data storage medium' (article 9/e).

2.4 **Offences related to infringements of copyright and related rights:**

The fourth category of cybercrimes under the Council of Europe's Convention on Cybercrime is 'offences related to infringements of copyright and related rights' (Section 1, title 4). This is because infringements of intellectual property rights, especially copyright, are among the most commonly committed offences on the internet. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent (ETS; 2001)

It should be noted that the Convention did not provide a definition of copyright and related rights, leaving this definition, consequently, on the national laws of member States.

List of additional material

Section Number 2 (Overview of Cybercrimes)

Section Title **The Categories of Cybercrimes**

Content Laws and Conventions:

The Council of Europe's Convention on Cybercrime, European Treaty Series - No. 185, Published 2001.

Explanatory Report to the Convention on Cybercrime; http://rm.coe.int/16800cce5b

The Jordanian Constitution (1952) page 3 of the Official Gazette (No 1093) dated 8 January 1952.

The Jordanian Cybercrime Law (No 27 of 2015) page 5631 of the Official Gazette (No 5343) dated 1 June 2015.

The Jordanian Penal Code, as amended (No 16 of 1960) page 374 of the Official Gazette (No 1487) dated 11 May 1960.

Content **References:**

Al-Nawaysa, Abdullah;*Crimes of Information Technology: Explanation of the Substantive Provisions in the Cybercrimes Law;*First Edition; Darwael for Publishing & Distributing; 2017; Amman; Jordan.

Content

Section Number **2(Overview of Cybercrimes)**

Section Title **Conclusion**

Content This chapter has provided an overview of cybercrimes by shedding light on a number of important issues regarding cybercrimes in three sections. In the first section, the question of what constitute a crime has been answered. In this regard, this section has indicated

that the expression 'cybercrime' is the most widely accepted expression used to refer to crimes committed through means of technology. Furthermore, this section has displayed definitions of the expressions used in the Jordanian Cybercrime Law, as it is important to understand what these expressions stand for. In the second section, this chapter addressed the three essential elements of a crime. These elements are: the legal element, the material element and the mental element. The third section has taken an in-depth look at categories of cybercrimes. In this respect, this section has studied the seven categories of cybercrimes stipulated under the Jordanian Cybercrime Law by naming these crimes, analyzing them and stating the punishments imposed for committing such crimes. This section also studied the categories of cybercrimes stipulated under the Council of Europe's Convention on Cybercrime.

Content Section Number **2 (Overview of Cybercrimes)**

Section Title **Table of Contents**

Content

Activity Template

Number	1
Title	Assess cybercrimes: elements and categories
Type	Reflection
Aim	Understand the major concepts related to cybercrimes, This activity relates to the following sections (2) The Elements of the Crime (3.1.5)The Fifth Category of Cybercrimes
Description	Read the following scenario of an act, then (working individually or in groups) assess whether this act is a crime, what are the elements thereto, and of which category. A one-page report should be submitted per answer
Timeline	Time: 0.5 hour
Scenario	Someone intentionally uses the internet to create a website to promote prostitution?
Assessment	**The student's answers can be reviewed according to the following model:** - This act falls under the fifth category of cybercrimes in accordance with the Jordanian Cybercrime Law which is the crime of sexual exploitation or prostitution-related crimes. - In this case, the main three elements of this crime have been achieved: 1- The first element is the legal element. This element can be found in Article 10 of the Jordanian Cybercrime Law which criminalizes and punishes promoting prostitution. 2- The second element is the material element in its three components: the *actus reus*, the criminal result and the causative relationship. 3- The third element is the mental element in its two components: the knowledge and the criminal will. - Consequently, as all the elements of the crime of sexual exploitation or prostitution-related crimes have been met, the commission for this crime will be subjected to the following punishments: imprisonment for a term not less than six months and a fine of 300-5000 Jordanian Dinars.

Activity Number	2
Title	**Assess cybercrimes: elements and categories**
Type	Reflection
Aim	Understand the major concepts related to cybercrimes This activity relates to the following sections (2) The Elements of the Crime (3.1.5)The Fifth Category of Cybercrimes
Description	Read the following scenario of an act, then (working individually or in groups) assess whether this act is a crime, what are the elements thereto, and of which category. A one-page report should be submitted per answer
Timeline	Time: 0.5 hour of reading.
Scenario	A student intentionally describes his colleague on one of students group on Facebook as a liar, rude and coward?
Assessment	**The student's answers can be reviewed according to the following model:** - This act falls under the sixth category of cybercrimes in accordance with the Jordanian Cybercrime Law which is the crime of electronic libel. This is because the student assaults the dignity and honour of his colleague without accusing him with a specific matter. - In this case, the main three elements of this crime have been achieved: 1- The first element is the legal element. This element can be found in Article 11 of the Jordanian Cybercrime Law which criminalizes and punishes the electronic libel. 2- The second element is the material element in its three components: A- The *actus reus*:describing his colleague as a liar, rude and coward. B- The criminal result: the violation of the interests that are protected by the law represented by violating the dignity and honour of his colleague. C- The causative relationship: describing his colleague as a liar, rude and coward resulted in violating his colleague dignity and honour. 3- The third element is the mental element in its two components: A- The knowledge: the student knows the nature of his behaviour. Furthermore, he knows that he is dealing with an electronic means. Additionally, he knows that the data or information sent includes something which harms the victim B- The criminal will: the student should not be forced to commit the criminal act. - Consequently, as all the elements of the crime of electronic libel have been met, the commission for this crime will be subjected to the following punishments: imprisonment for a term not less than three months and by a fine of 100-2000 Jordanian Dinars.

Think (MCQs) Chapter 2 Overview of Cybercrimes

Number 1

Title What Constitutes a Crime

Type Multiple choice question

Question What is the most common expression used in the literature to describe crimes committed using technology?

Answer **A- Cybercrime**

B- Computer Crime

C- Internet Crime

D- Digital Crime

Think (MCQs) Chapter 2 Overview of Cybercrimes

Number 2

Title What Constitutes a Crime

Type Multiple choice question

Question **Which one of the following expressions is not explicitly defined under the Jordanian Cybercrime Law?**

Answer A- Data
B- Information System
C- Cybercrime
D- Website

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 3
Title **The Elements of the Crime**
Type Multiple choice question
Question **Which one of the following is an element of any crime?**
Answer A- The legal element
B- The material element
C- The mental element
D- All of the above

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 4
Title **The Elements of the Crime**
Type Multiple choice question
Question **Which of the following is a requirement for establishing a criminal offence under the principle of legality?**

Answer A- Custom
B- Written rule/rules
C- Habit
D- None of the above

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 5
Title The Elements of the Crime
Type Multiple choice question
Question **Which of the following is considered a part of the material element?**

Answer A- The act
B- The criminal result
C- The causative relationship
D- All of the above

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 6
Title The Elements of the Crime
Type Multiple choice question
Question **Which of the following is known as the *actus reus*?**
Answers **A- The act**
B- The criminal result
C- The causative relationship
D- The criminal will

Think (MCQs) Chapter 2 Overview of Cybercrimes

Number 7

Title The Elements of the Crime

Type Multiple choice question

Question **The causative relationship in the material element is represented by:**

Answer A- The relationship between the actus reus and the mens rea

B- The relationship between the actus reus and the criminal result

C- The relationship between the mens rea and the criminal result

D- The relationship between the mens rea and the criminal will

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 8
Title **The Elements of the Crime**
Type Multiple choice question
Question **The mental element, in any crime, is known as?**
Answer A- The actus reus
B- The mens rea
C- The criminal result
D- The criminal will

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 9
Title **The Elements of the Crime**
Type Multiple choice question
Question **What are the components of the mental element?**

Answer A- The actus reus and the criminal result
B- The causative relationship and the criminal result
C- The knowledge and the criminal will
D- None of the above

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 10
Title **The Categories of Cybercrimes**
Type Multiple choice question
Question **The crime of illegal access to the internet requires the following?**
Answer A- The legal element
B- The material element
C- The mental element
D- All of the above

Think (MCQs) Chapter 2 Overview of Cybercrimes

Number 11

Title **The Categories of Cybercrimes**

Type Multiple choice question

Question **The publishing component in 'the crime of illegally using a program in order to achieve an illegitimate purpose' means**

Answer A- Adding programs by using the internet or information system

B- Distributing programs by any means using the internet or information system

C- Utilizing data or a program

D- None of the above

Think (MCQs) Chapter 2 Overview of Cybercrimes
Number 12
Title **The Categories of Cybercrimes**
Type Multiple choice question
Question **Which of the following is considered a computer-related offence under the Council of Europe's Convention on Cybercrime?**

Answer **A- <u>Computer-related fraud</u>**
B- Illegal access
C- Illegal interception
D- Data interference

Extra: Chapter 2 Overview of Cybercrimes
Number 1
Title **Principles of Cybercrime**
Topic **What Constitutes a Crime**
Type Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2015).

Extra: Chapter 2 Overview of Cybercrimes

Number 2

Title **Explanation of Criminal Law General Section: Analytical Study in General Theory for Crime and Penal Liability**

Topic **The Elements of the Crime**

Type Nitham T. Al-Majali, *Explanation of Criminal Law General Section: Analytical Study in General Theory for Crime and Penal Liability* (Arabic edn, 5th edn, Dar Al-Thaqafa for Publishing & Distributing 2015).

Extra: Chapter 2 Overview of Cybercrimes

Number 3

Title Explanation of the Substantive Provisions in the Cybercrimes Law

Topic **The Categories of Cybercrimes**

Type Abdullah Al-Nawaysa, Crimes of Information Technology: Explanation of the Substantive Provisions in the Cybercrimes Law (Arabic edn, 1st edn, Darwael for Publishing & Distributing 2017) 213, 219.

3. Admissibility and credibility of evidence in digital issues

Scope
Number 3
Title Admissibility and credibility of evidence in digital issues
Introduction This chapter will address the concept of digital evidence, explaining the authorities that have the power to extract analyze and present digital evidence, and to whom, as well as the conditions for admissible and credible digital evidence.
Outcomes The students will be able to understand the following:
- The concept and importance of evidence in a legal setting.
- The different roles played by the three main authorities in establishing what constitutes legal evidence.
- The role of PSD, GPD and judicial officials in conducting investigation.
- The conditions that make evidence admissible and credible in courts.

Study Guide

Task	Time
Preparation (Introduction and On-line Planning):	1.5 hrs
Textbook Content:	4 hrs
Thinking (online discussion review questions)	1.5 hrs
Tutorial Work on Law and Legal Systems	1.5 hrs
Related Course Work	1.5 hrs
Total	10 hrs

Required external resources:
- PSD; the Jordanian Public Security Department; Guide for Investigating Electronic Crimes; file:///C:/Users/user/Documents/FORC/resources/%D8%AF%D9%84%D9%8A%D9%84%20%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9.pdf
- PSD; the Jordanian Public Security Department; Training manual for dealing with digital evidence; file:///C:/Users/user/Documents/FORC/resources/الادلة%20الرقمية.pdf
- National Institute of Justice; Forensic Examination of Digital Evidence: A Guide for Law Enforcement; U.S. Department of Justice; Office of Justice Programs.file:///C:/Users/user/Documents/FORC/resources/US-digital-forensics.pdf
- Digital forensics and crime; The Parliamentary Office of Science and Technology, London; 2016. file:///C:/Users/user/Documents/FORC/resources/uk-report.pdf

Chapter 3 Admissibility and credibility of evidence in digital issues

Author **Lina Abdallah Khalil Shabeeb,**
Associate Professor of Public Law, School of Law, University of Jordan

Section Number 3
Section Title **Admissibility and credibility of evidence in digital issues**
Introduction This chapter will address how and by whom digital evidence is found and presented in a formal setting, especially in a court of law, in a manner that makes it reliable and trustworthy, i.e. admissible and credible. This is presented in three sections; first, the concept of evidence in general is presented; especially what is perceived as legal (i.e. admissible and credible) evidence, and the general conditions thereof. Second, the authorities responsible for finding digital evidence is presented, arriving at the Unit for combating Electronic crimes at the Public Security Department. The third section will address the process of investigating digital crimes and the principles thereof.

Content

Content

Section Number 3

Section Title **Legal Evidence in General**

Introduction Evidence may be defined as the "available body of facts or information indicating whether a belief or proposition is true or valid" (Oxford Dictionary). In other words, evidence is what a party uses to proof its claim; this can take different shapes and forms and can be presented in different settings. In a legal setting, in general, the importance of the principles of proof and evidence lies in forming the judges' final decision in the dispute at hand, therefore it is of utmost importance to implement the provisions of evidence with precision and in a proper legal manner.

In a legal setting, the laws of evidence provide the general principles that govern evidence; however, there is some difference in some aspects of evidence in a civil (non-criminal) setting as opposed to a criminal setting. This is especially clear in the end result of presenting evidence, in a civil setting, the objective of evidence is to prove a party's right, which can always be translated into monetary rights; in a criminal setting, however, the role of evidence is noticeably different, the freedom (or even life) of a person sometimes depends on evidence.

Before further explaining the types and principles of evidence, it must be noted that one of the most crucial aspects of evidence is the burden of proof of the evidence which "means that in general the party that cites specific facts for the substantiation of its claim also has the burden of producing the evidence to prove these facts. This burden depends on the substantive law governing the claim. Permissible presumptions and legal rules can shift the burden in various situations."

In a criminal setting, the burden of proof lies on the public prosecutor, although the accused can present his/her evidence, some evidence can only be seized and presented by the public prosecutor, especially in digital crimes.

In a civil setting, the judge or arbitrator's discretion in weighing evidence is limited by the governing laws, in addition, his/her role is to weight the evidence presented by competing parties to assert their claims and rule accordingly. In a criminal setting, the court's discretion is wider because the ultimate purpose is establishing innocence or guilt based on facts and evidence, and without reasonable doubt.

Hence, in a legal setting, and as far as legal evidence is concerned, there are differences between criminal and civil cases, as follows

Content

1. **Types of evidence**

Typically, the concept of legal evidence and the role it plays in courts is the same in a legal setting, whether civil or criminal, however, conceptually, there is an obvious difference in providing evidence between civil and criminal cases. Simply, it is quite different to prove a monetary right than to prove that a crime is committed; the consequences are obviously divergent. However, the general principles in addressing the courts and the relevance of the facts to be proven are the same in a legal setting, be it civil or criminal.

1.1 **Evidence in Civil Proceedings**

To begin with; principles of legal evidence can be divided into two sections: procedural principles and subjective principles. Procedural principles regulate the means of handling the evidence and the steps that must be followed in examining the evidence in court. On the other hand, subjective principles are the rules that determine the admissibility of the evidence, the burden of proof, and its significance in the case at hand.

The Jordanian legislator listed six types of legal evidence in Article 2 of the Jordanian Evidence Law (no. 30 for the year 1961) as follows (the equivalent article in the Palestinian Law of Evidence in Civil and Commercial cases, no. 4 for the year 2001, is article 7):

1. Written Evidence
2. Witness Testimony
3. Presumptions
4. Experts Opinions

5. Declarations
6. Oath

The above mentioned evidence can be divided into direct evidence and indirect evidence. Direct evidence is simply that is related directly to the fact concerning to the dispute at hand. Written evidence, witness testimony, and expert's opinions are considered direct means of proof. While the rest of the evidence are considered indirect, meaning that facts can be deducted using them.

1.2 **Evidence in Criminal Proceedings**

Proof under the provisions of criminal proceedings may be defined as: providing evidence to prove whether a crime is committed or not, and if so proving the facts that connect the criminal act to a perpetrator. The general principle in criminal trials is that the person is innocent until proven otherwise; in order to prove the guilt or innocence of a person certain rules must be followed.

Types of evidence in criminal proceedings differ from those previously outlined in civil proceeding. The following types of evidence are relied upon in criminal cases:

1. Confessions
2. Witness testimony
3. Experts opinions
4. Written evidence
5. Presumptions

However, according to article 147 of the Jordanian Criminal Procedures Law (article 206 of the Palestinian Criminal Procedures Law): "Proof in felonies, misdemeanors and infractions shall be established by all means of proof and the judge shall rule according to his personal conviction (i.e. the court's discretion)" (Saeed, K. 2005)(Abdelbqi, M., 2015).

In digital crimes, most of evidence is presented by the judicial officers liaised with the Unit for Combating Electronic Crimes, through a document referred to as the 'technical report', which the court can (or shall) relay on(article 150 of the Jordanian Criminal Procedures Law and article 212 of the Palestinian Criminal Procedures Law); as will be illustrated in the third section.

Note: The types of evidence in both Jordanian and Palestinians laws are not provided in one article as in Evidence law in civil cases, those types are concluded from several articles in both, the Jordanian Criminal Procedures Law no. 9 for the year 1961 and the Palestinian Criminal Procedures Law no. 3 for the year 2001.

2. **Relevance of Evidence**

After addressing the types of evidence as listed in the Jordanian law, a look must be taken on the facts that are meant to be proven. There are four conditions that must apply to these facts; two of which are listed in the Evidence Code while the other two were deduced by scholars (Mansour, A., 2015). These conditions are:

1. The fact must be related to the issue at hand.
2. The fact must affect the decision of the judge (productive fact).
3. The fact must be legally accepted and does not infringe Public Order.
4. The fact must be specific and concise.

Hence, in both civil and criminal cases, evidence must be relevant to the case at hand. In the upcoming sections, the principle guiding what constitutes good evidence will be explored, however, before establishing how good a piece of evidence is, and before putting the effort to make it admissible and credible before courts, a preliminary assessment should take place, which is: how relevant this evidence is? Or what is the significance of the fact at hand to the issues being proved. The relevance test is usually conducted by law professionals rather than technicians and digital experts; therefore, the technical team should treat each piece of fact as equally important and relevant until reviewed by the legal team.

3. **Digital Evidence**

The concept of evidence in digital cases is not different from what was provided previously; however, digital evidence proved to be more challenging than other types of evidence, whether in civil cases, or, more importantly, in criminal cases. Digital evidence tends to be more voluminous, more difficult to destroy, easily modified,

easily duplicated, potentially more expressive, and more readily available (Ryan, D.J. Retrieved 25 May 2019). The world is rapidly becoming digital and not all stakeholders are keeping pace; unfortunately, criminals and persons with mal intentions move faster than concerned officials. Hence there is always a problem with the availability of expertise. Forensic science relies on testing and verification, therefore, constant change pose a problem: 'The problem for those operating with information technology is the rate of change - DNA doesn't change, but computer hardware, operating systems, application programs do - dramatically over periods as short as five years' (Sommer, P., retrieved 25 May 2019).

Providing evidence in digital cases has several other challenges in different aspects; the most important of which is how to present digital evidence to courts? In other words: how to make law professionals understand the technicalities of the digital evidence? Or how to make law professionals understand digital jargon? More importantly, the question being addressed by this book: how to make IT experts understand legal jargon.

This is equally applicable in civil as well as criminal settings; however, in a criminal setting, providing digital evidence is more challenging. The second chapter of this book addressed the concept of crime and the elements thereof; this chapter is presenting the concept of evidence and how to prove (in a court room) whether or not a crime is committed, and more importantly, how to connect this crime to the suspect. The previous chapter presented that a crime has three elements: the legal element, the material element and the mental element. The investigator's role in digital crimes is to provide evidence for all or some of those elements (Maghaireh, A., 2009)

For example, in the crime of digital blackmail, first, the act of digital blackmail should be criminalized either in the penal code or in the cybercrimes law: the legal element. The investigator's role here is to determine whether the act carried by the perpetrator mounts to the crime presented in the law; i.e. does this act, no matter how malicious it is, constitute a crime as described by the law? And of course: which crime? And what are the surrounding circumstances of committing this criminal act. Second, the investigator should establish the material element, i.e. the act of digital blackmailing and how it took place; as presented in the previous chapter, this includes three other components: the act, the result (mal effect of the criminal act), and the causative relation between those two components: the act and the result. In the crime of digital blackmail, the investigator must provide evidence of the act that constitutes digital blackmail (i.e. and email that is sent by the perpetrator and linked to his IP address, or, simply, from his/her email), and how this act is connected to the victim affecting him badly (i.e. proof that the email reached the victim is digital) and how it affected him. The third element is the mental element, which is quite challenging for the investigator to prove, hence he/she must provide all the evidence thereto, such as a pervious (related) emails from the perpetrator, or the fact that the perpetrator did some search on the victim to gather data about him that was used later in the act of digital blackmail.

Note: it should be noted that the surrounding circumstances of committing the criminal act will affect the court's discretion, because in law, some circumstances could affect the judge to either elevate or reduce the sentence.

List of additional material

Section Number	3
Section Title	**Admissibility and credibility of evidence in digital issues**
Content	Abdelbaqi, Mustafa; The Palestinian Criminal Procedures Law, A Comparative Study; (text book); Birzeit University; August 2015; Palestine; https://fada.birzeit.edu/bitstream/20.500.11889/5464/1/%288-5%29.pdf

Maghaireh, Alaeldin Mansour Safauq; Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence; University of Wollongong; 2009; https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4404&context=theses

Mansour, Anees; An explanation of the Jordanian Law of Evidence; Second Edition; Ithraa Publishing and Distribution; 2013; Amman; Jordan.

Ryan, Daniel J. and Shpantzer, Gal; "Legal Aspects of Digital Forensics" (PDF); http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf

Saeed, Kamel; the Law of Criminal Proceeding, a comparative and analytical study; (text book); Dar Al-Thaqafa; 2005; Amman; Jordan.

Sommer, Peter; Emerging Problems in Digital Evidence; https://www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/09627250408553241.pdf

Content Section Number 3

Section Title **Investigating authorities**

Introduction Investigating digital evidence is usually related to criminal investigation, in the sense that, in a civil setting each concerned party will present the evidence that support their claim and the court's role is to weight this evidence and balance the weight of evidence between disputing parties.
In digital crimes, as in other crimes in Jordan (same in Palestine, according to article 1 of the Palestinian Criminal Procedures Law), the investigation authorities are only in the public domain, even if, as in most digital crimes, this investigation is initiated by a complaint, the complainant does not have the right to investigate the act he/she is complaining from, only the relevant public authorities have this power.

Content

1. **Different authorities with different roles**

As presented in chapter one, governance is divided between three powers, Legislative, Executive and Judicial; all play an important role in regulating and conducting investigation in digital cases. The Legislative Power issues all relevant laws regarding digital issues, especially digital crimes, starting from criminalizing malicious acts, to investigating crimes, until such acts are punished by courts. Such courts are different criminal courts in Jordan, which are part of the Judicial Power. The Executive Power also plays an important part in combating digital crimes; the Public Security Directorate PSD (The equivalent in Palestine is the Police in the National Security Forces), which is directly connected to the Ministry of Interior Affairs, is the main authority that takes charge of fighting and preventing crimes in general, and digital crimes in particular, in Jordan.

2. **The Legislative Authority**

This authority has issued many laws that are relevant to criminalizing and investigating digital crimes; some of those laws are:
General Jordanian Laws:
- The Pinal Code no. 16 for the year 1960.
- The Evidence Law no. 30 for the year 1952.
- The Criminal Procedures Law no. 9 for the year 1961.
- The Banking Law no. 28 for the year 2000.
- The Securities Law no. 18 for the year 2017.
- The Law for Public Security no. 38 for the year 1965.

In Palestine, the relevant laws are:
- The Jordanian Penal Code no. 16 for the year 1960.
- The Evidence Law in Civil and Commercial cases no. 4 for the year 2001.
- The Criminal Procedures Law no. 3 for the year 2001.

- The Law for the Formation of Ordinary Courts no. 5 for the year 2001.
- The Law of Communications no. 3 for the year 1996.
- The Securities Law no. 12 for the year 2004.
- The Consumer Protection Law no. 21 for the year 2005.
- The Law for Combatting drugs no. 18 for the year 2015.

Digital Laws in Jordan:

- The Law of Electronic Crimes no. 27 for the year 2015.
- The Law for Electronic Transactions no. 15 for the year 2015.

Digital Laws in Palestine:

- The Palestinian Electronic Crimes Law no. 16 for the year 2017.
- The Palestinian Law for Electronic Transactions no. 15 for the year 2017.

3. **The Judicial Authority**

The main responsibility of the judicial branch is to resolve disputes by applying the Jordanian legislation on matters at hand. "An effective judiciary system recognizes the value and importance of integrity and equality, as well as the value of establishing equal opportunities and maintaining the rights and liberties of citizens as stated in Jordan's Constitution and as guaranteed by the country's rules and regulations." Articles 97 through to 102 of the Jordanian constitution embedded the principles of the independence of judges and the hierarchy of Courts in the Kingdom; article 97 of the Jordanian Constitution provides that: "*Judges are independent and, in the exercise of their judicial functions, are subject to no authority other than that of the law*."

According to article 99 of the Jordanian Constitution, the courts shall be divided into three categories: Civil Courts, Religious Courts and Special Courts. Crimes and criminals are referred either to ordinary criminal courts or to special criminal courts; the body that refers such cases to criminal courts is another judicial body embodied in the General Prosecutorial Department GPD.

The Palestinian legal system has a very similar judicial structure, provided in the Law for the Formation of Ordinary Courts no. 5 for the year 2001.

3.1 **Courts**

Digital evidence is customarily presented before courts by disputing parties, and the court might use expertise in this matter, to create its conviction; however, presenting digital evidence before criminal courts is more challenging and can only be presented by formal authorities, as follows.

A. Ordinary Criminal Courts or Regular Courts are:

1.Conciliation Courts: These courts hear all violations, crimes involving perjury and false oaths arising from conciliation cases, and misdemeanors punishable by law with a prison term not exceeding two years, except misdemeanors perpetrated against state security, and misdemeanors for which a special provision states that courts other than the conciliation courts shall hear them (Article 5 of the Conciliation Courts Law).

2.Courts of First Instance: these courts hear misdemeanor cases that are outside the jurisdiction of the conciliation court. In addition to criminal cases that fall outside the jurisdiction of the superior criminal court pursuant to its law (Article 5 of the Law Regarding the Composition of Regular Courts) and in misdemeanor cases associated with the felony referred to them in accordance with the indictment (Article 14 of the Criminal Procedure Code).

Such courts also act as courts of appeal for Conciliation Courts, hence they hear the cases appealed before them against certain judgments rendered by the conciliation courts, which involve imprisonment for violations, misdemeanor imprisonment for a period not to exceed one month or a misdemeanor fine not to exceed thirty dinars (Articles 5 of the Law Regarding the Composition of Regular Courts and 28 of the Conciliation Courts Law).

3.Courts of Appeals: these courts hear all judgments rendered by courts of first instance, in their capacity as first instance and criminal courts with respect to felonies, misdemeanors and violations, as well as judgments and decisions for which there is a special provision stated in any other law that allows for the appeal thereof (Article 256 of the Criminal Procedure Code).

4.The Court of Cassation, which is the superior court in Jordan.

B. **Special Criminal Courts, which include:**

1. Superior Criminal Court, which hears the following crimes: murder crimes, crimes involving rape, indecent assault, and criminal kidnapping; in addition to the attempt to commit those crimes.
2. Police Court, which hears crimes committed by persons affiliated with public security.
3. Juvenile Courts, which hear charges attributed to any juvenile.
4. Military Courts, which hear any case involving crimes committed by military personnel, whether military or ordinary crimes.
5. State Security Court, which hears only four types of offences: high treason, espionage, terrorism, and drug trafficking.
6. Customs Courts, which hear custom crimes.

3.2 **The General Prosecutorial Department GPD**

Courts with criminal jurisdiction are assisted by theGeneral Prosecutorial Department GPD, which is a judicial body, yet it is completely independent from all bodies of the government. This is considered one of the most important principles that ensure integrity and reliability in criminal proceedings. In addition, one of the important legal facts is that general and public prosecutors are perceived as fair opponents, this is because they look for evidence of innocence and guilt equally as their purpose is not to blindly prosecute perpetrators, but to look for justice and restore the public rights of people and public order.

Note: There is an equivalent authority in Palestine, with a very similar structure, system and role(article 1 of the Palestinian Criminal Procedures Law).

The GPD is headed by the Head of Public Prosecution, with several General Prosecutors in different courts and General Prosecutor assistants as well as Public Prosecutors, spread all over courts and judicial bodies in Jordan. Most criminal courts in Jordan must have a member of the General Prosecutorial Department (article 14 of the Jordanian Law of Formation of the Regular Courts and its Amendments No. 17 of 2001);their role is to "establish and pursue criminal proceedings as set forth in the Code of Criminal Procedure and other laws" (article 15). The latter law provides (in article 2) the main role of GPD, which "have the power to start and exercise the prosecution of crimes; the initiation of the criminal proceedings shall only be done by the public prosecution (and any other body which is given such power according to the law)."

Accordingly, criminal offences must first pass by the GPD before being referred to the proper court. The GPD is presented by the public prosecutors (at different levels) whom examine the offences, look for evidence and perpetrators then decide whether or not to refer the matter to the criminal court.

The public prosecutors, after being informed about a criminal offence, begin to look for evidence and possible perpetrators of the offence, accordingly if enough data was gathered they refer the offence to the competent courts. The main purpose of a criminal trial is to prosecute the perpetrator, defend the public right and restore public order, as a criminal offence is thought to be an infringement to the public right of the people and the general public order, rather than just a violation of the personal rights of individuals or mainly victims, who also, in some instances, can take their cases to the criminal courts on their own; however, if a criminal case is established before a court, victims have the right to give up or droptheir personal right in a criminal offence, the public right is not dropped and the criminal proceedings still take place.

In their search for criminal acts, evidence and perpetrators, the GPD is assisted by another body referred to as the Judicial Officers, who usually conduct the first acts of investigation, either on their own, or, as in the majority of cases, according to the directions of the GPD members or Judges. Many officials have the title of a Judicial Officer, which gives them distinctive power, the most important of which is the right to inspect crimes and hold perpetrators or property (temporarily until trial). All judges and all GPD Prosecutors have the capacity of judicial officers; however, most judicial officers are public security personnel (police) and are affiliated with the Public Security Directorate, an independent body that is directly connected to the Ministry of Interior Affairs.

The GPD may, within its jurisdiction, request the assignment of any officer of the police as a judicial officer to perform the functions of the prosecution in the courts of first instance and of the general or temporary courts as may be required and the managing officer has to comply with instructions issued to him by the Attorney General Or the Prosecutor (article 15/b of the Jordanian Law of Formation of the Regular Courts). The managing officer, or the staff of the judicial police, for that matter, shall be subject to the supervision of the GPD in respect of their judicial functions (article 18).

4. **The Executive Authority**

This authority have many units that are directly involved in combating and investigating digital crimes, many governmental bodies have judicial officers in their system to assist in combating and investigating crimes against public order in the domain of such bodies (whom are directly linked with the GPD). However, the main governmental institute that is in charge of fighting crime and that recruits (and trains) judicial officer is the Public Security Directorate PSD.

4.1 **The Judicial Officers (or Police)**

The Jordanian law of criminal procedures, under the title of Judicial Police, provides that "members of the Judicial Officers Corps are required to seek out information and conduct the preliminary investigation of the crimes in addition to the collection of evidences and the arrest of the perpetrators of such crimes in order to refer them to the competent courts which have the authority to punish them" (article 8). It also provides that the public prosecutor shall be assisted in his/her judicial policing functions by: administrative governors, the director of public security, police directors (chiefs), heads of security centers, police officers and members, officials who perform criminal investigation duties, mokhtars (local communities' chiefs) and captains of sea and air ships (article 9).

Palestine has a very similar police system, where judicial police carry such duties (article 19/2 of the Palestinian Criminal Procedures Law).

4.2 **The Public Security Directorate (PSD)**

Figure (1): The Public Security Directorate

This body is the main governmental body that is in charge of fighting crime by conducting many duties (article 4 of the Jordanian Law for Public Security no. 38 for the year 1965), the most important of which are the "preservation of order and security and the protection of lives, honor and properties," the "prevention of crimes and endeavor to discover and pursue them, to arrest and apprehend their perpetrators and deliver them to justice," as well as "the implementation of laws and regulations, judicial and legitimate orders, and assisting the Public Authorities in executing their functions according to the stipulations of laws."

PSD has many departments that conduct different roles; the General Director's Assistant for judicial affairs is in charge of many departments that play an important role in fighting crimes in Jordan, one of which is the Forensic Laboratory Department. The Criminal Investigation Department also plays an important role thereto, to which the main unit in combatting digital crimes is affiliated, which is the Unit for Combating Electronic Crimes. Almost all personnel of those departments have the power of judicial officers in conducting their duties, which gives them, as presented earlier, an important investigative role.

4.3 **The Unit for Combating Electronic Crimes**

This Unit is one of the units that are affiliated with the Criminal Investigation Department; it is the main body in charge of investigating digital crimes, to which it has its own specialized labs (in addition to the labs at the Forensic Laboratories Department).

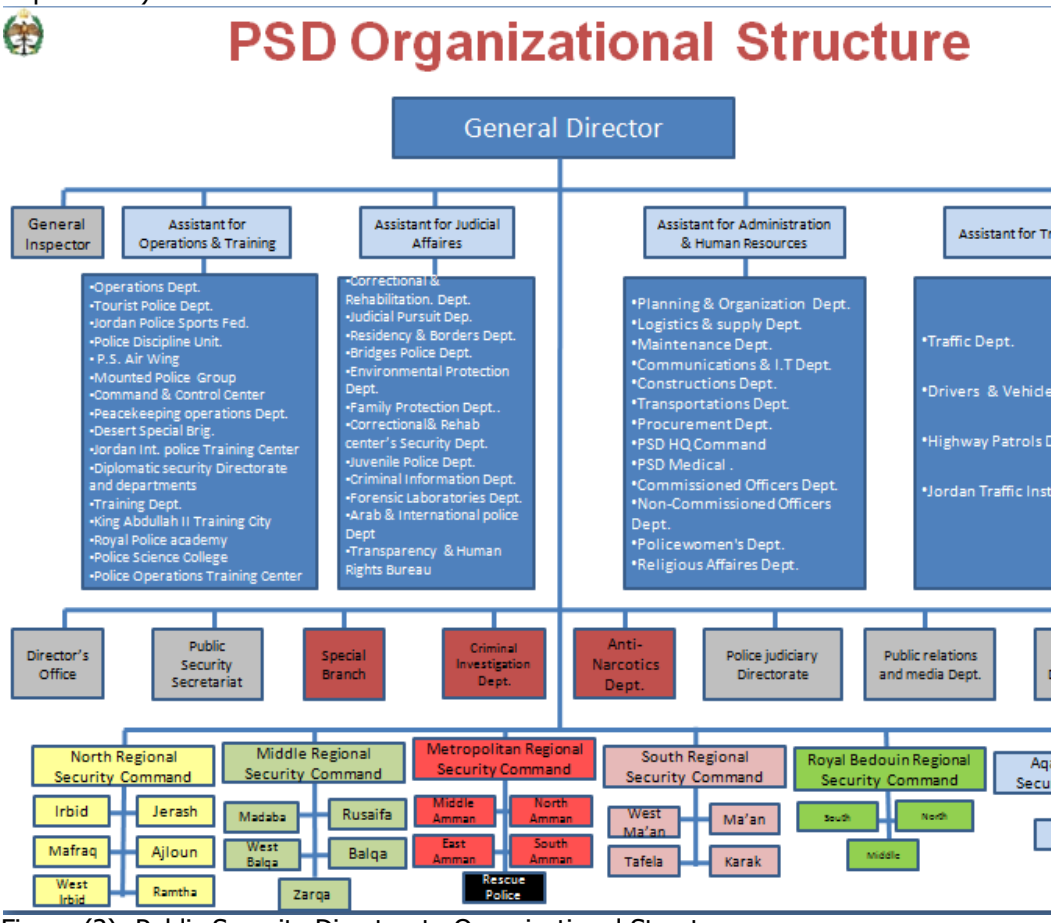


Figure (2): Public Security Directorate Organizational Structure.
Source: https://www.psd.gov.jo/index.php/en

This unit recruits judicial officers who are well-trained to deal with digital crimes, which are referred to them either by the GPD or by direct complaints from the victims.

Note: The Unit for Electronic Crimes in Palestine was established in 2013 to carry out a very similar role to the one presented above.

Content

Section Number 3

Section Title **Investigating digital crimes**

Introduction Digital crimes, like other crimes, must be investigated using the general principles of investigation, and must be conducted by the formal authorities in charge. However, digital evidence is somewhat different from other evidence, hence, needs a different approach from investigative authorities.

Proving digital crimes is quite challenging, the challenges are numerous and multifaceted, yet, most of these challenges are encapsulated in ensuring the reliability of evidence in a formal or legal setting, which is referred to as the **admissibility and credibility of evidence** before a court, in other words: 'how to make digital evidence admissible and credible before courts?'

This section will attempt at answering this question by presenting the different stages of investigation, the formalities for preparing the 'technical report' and the principles governing investigating digital crimes and extracting evidence and the processes by which this is done: tools, steps and chain of custody.

Content

1. **Investigation stages**

Customarily there are three stages of investigation, the first stage is inspecting and gathering information (assessing whether or not a crime is committed), the second stage is called the preliminary investigation stage (where there is a formal investigation of the criminal act and the suspected perpetrators) and the third stage called the final investigation stage, which is primarily conducted (and partly directed) by the presiding judge and takes place during the trial (Keelany, F., 1995, p. 17).

The judicial Officers carry out the inspection of crimes, based on one of three actions: (1) a formal complaint from the victim, (2) information of the public or other sources or (3) by assignment of the Prosecutor General.

The inspection of suspicious acts is a process of exploring if a crime is committed, accordingly, the GPD decides whether or not there is a need to conduct a preliminary investigation, which is carried out using different investigative methods; some of which are searching, inspection, examination, interviews, interrogations, evidence collection and preservation or confiscation. All such measures must be conducted by a formal order (e.g. search warrant) of the GPD; especially arresting a suspect, and/or searching private property. The preliminary investigation is a serious process, by which the Public Prosecutor decides either to dismiss the case, or to refer it to the relevant criminal court; hence, it is considered to be the first step of the criminal trial, by which, the Public Prosecutor's role is to determine if a crime is committed, which crime, whether it's a felony or a misdemeanor, connecting the suspect to the crime and most importantly: the evidence thereto.

The final investigation is the last stage, which is conducted by the court; therefore, the process of such investigation is quite different from the preliminary investigation. The court's role is mainly based on weighing the evidence and assessing the connection of the suspect to the crime.

Those stages of investigation are guided by several principles to guarantee the admissibility and credibility of evidence before a court, as will presented hereunder.

Note: Palestine applies a very similar system of investigation, embodies in its relevant laws, especially the Palestinian Law for Criminal Procedures.

2. **Formalities of the technical report**

As provided earlier, most of the digital evidence is presented via a technical report (article 147 of the Jordanian Criminal Procedures Law; and article 212 of the Palestinian Criminal Procedures Law), organized by judicial officers usually working at the Unit for Combatting Electronic Crimes. For such reports to be admissible (and credible) they must fulfill the flowing conditions(article 151 of the Jordanian law and article 213 of the Palestinian law):

1. Reports must be composed within the judicial officer's jurisdiction (authority), and this must take place while performing the functions of his/her post.

2. Reports must be composed by the judicial officerwho personally investigated the incident or who was personally notified thereof.
3. Reports must fulfill all legal formalities provided in governing laws.

3. **Extraction of digital evidence**
Extracting digital evidence is usually carried out using the following steps (PSD, Training Manual, retrieved April 2019):
1. Evidence identifying: which means that the investigator identifies that what he/she has at hand could constitute digital evidence, and where and how it was stored.
2. Evidence safekeeping: this means the measures taken to safeguard digital evidence, and to preserve it from contamination or interference, i.e. preventing any change of its contents and/or stored data (as part of the chain of custody).
3. Evidence analysis: this means that the data in digital evidence is extracted and interpreted in a way that is comprehensible to most people (in layman language).
4. Evidence presentation: this means presenting the digital evidence (in the technical report) to the competent court, during the court's hearings and within its procedures.

4. **The process of and the tools for extracting and documenting digital evidence:**
Conducting investigation of digital crimes involves the following tools and processes (PSD, Guide, retrieved March 2019):
4.1 **Tools**
The unit for combating electronic crimes has its own forensic lab to extract and examine digital evidence. Several tools can be used to conduct forensic investigation of digital evidence, some of which are as follows: a digital intelligence station (toolkit) that uses Encase 6.18.1 and FTK, Cellebrite digital forensic toolkit (used to investigate mobile phones), portable disc, and much other forensic programs, software and suite, such as: Oxygen, password cracking, e-mail tracking, IP address tracking and IP address hide software, computer search warrant program, X-Tree Pro Gold program, Lab link program, view Disc program, LanTastic program and some other tools.
4.2 **Steps**
The process used for digital evidence extraction starts by using the appropriate hard disc drive (data, power) depending on the hard disc type (SATA, IDE, SCSI), then connecting the hard disc to the Write Blocker (to preserve the date), then taking a Physical Image of the hard disc, then performing the data analysis (according to the case at hand) and placing results in relevant folders, then copying the results on a CD-ROM (or a similar tool), and finally, printing out copies to attach to the technical report (the National Institute of Justice, retrieved May 2019).
4.3 **Documentation (chain of custody)**
Good evidence stand in court, in other words, all the hard work the investigators carry out in extracting, collecting, analyzing, reporting and presenting digital evidence must be properly documented. The concept of the chain of custody applies to all sorts of evidence; it means the chronological documentation of evidence, from the first instance of investigation (the search warrant) until presenting the evidence in court. Digital chain of custody is especially important due to the vulnerability of digital evidence, bearing in mind that the defendant has the right to rebut such evidence presented in the 'technical report' using all available means of proof (article150 of the Jordanian Criminal Procedures Law).
The chain of evidence in investigating digital crimes indicates the collection, sequence of control, transfer, and analysis of evidence. It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. In short it proves impartiality and control:
"One element often overlooked in the rush to obtain evidence during a forensic investigation is control. To prove impartiality you must be able to answer the five W's and H questions: who, what, why, when, where and how. Who controlled the evidence? What was used to collect it? Why was it done in that manner? When was each piece of evidence found? Where was the evidence found? How was it

documented? Ultimately, if the chain of custody (also referred to as the chain of evidence) is not maintained, all evidence can be challenged and thrown out of court (Cobb, CH., retrieved March 2019)."

The documentation of evidence during the investigation of digital crimes includes all related evidence and not only digital evidence. One of the important evidence that must be properly documented is the testimonies taken during the investigation; such documented testimony should include all related technical data, for example, writing the domain/or and e-mail address accurately, the time and date of the testimony (or complaint), and which type of digital crime is at hand.

The documentation in digital investigation includes writing several reports; such as the examination report, e.g. in email related crimes, this includes the steps before acquiring the password to accessing the email, the time and date, what was observed, where was the link, then printing out the content and taking an image of the screen. There is also the inspection report, the transfer report and the suspect (if any) identification report (PSD, Guide, retrieved March 2019) (Digital forensics and crime, 2016, retrieved May 2019).

5. **Ethics**

Just like all other professions, investigators in particular and judicial officers in general, should carry out their work under the umbrella of professional ethics. Many scholars discus the traits that a good investigator must have (Saeed, K., 2005, p. 423), such as patience, attention to details, tranquility, highly organized, quick response, observant and so on; however, one must distinguish between the characteristics, skills and ethics of investigators. Evidently, all are important qualities a good investigator must have; nonetheless, the ethical part of this profession is the most important one. The ethics an investigator must have are somewhat similar to the ethics of a judge; in the sense that, as provided earlier, the investigator, and the public prosecutor for that matter (whose main role is to incriminate the suspect before courts) are not enemies of the suspect, they are perceived as an honest opponent merely seeking the truth rather than seeking conviction.

Amongst many ethics persons in law enforcement must have, the following are essential: objectivity, integrity, confidentiality, sincerity, fidelity, accountability, fairness, independence (i.e. not influenced by other than seeking the truth) morality and good conscience. The investigator must bear in mind that he/she will, at some stage in the case at hand, provide testimony to his/her report before the court (Garrie, D.B., retrieved April 2019); where the court, the victim, the suspect as well as the public order depend on this testimony.

List of additional material

Section Number	3
Section Title	**Admissibility and credibility of evidence in digital issues**
Content	Cobb, Chey; How to secure the chain of custody in a digital forensics investigation; https://searchitchannel.techtarget.com/tip/How-to-secure-the-chain-of-custody-in-a-digital-forensics-investigation Digital forensics and crime; The Parliamentary Office of Science and Technology, London; 2016. file:///C:/Users/user/Documents/FORC/resources/uk-report.pdf Garrie, Daniel B. and Morrissy, J. David; Digital Forensic Evidence in the Courtroom: Understanding Content and Quality; Northwestern Journal of Technology and Intellectual Property; Volume 12; issue 2; Spring 2014; file:///C:/Users/user/Documents/FORC/resources/Digital%20Forensic%20Evidence%20in%20the%20Courtroom_%20Understanding%20Content.pdf

Keelany, Farouq; Lectures in the Law of Criminal Proceedings in Jordan and comparative law; (text book); 2nd part; third edition; Eastern Publication Inc.; Dar Almorouj; 1995, Beirut; Lebanon.

National Institute of Justice; Forensic Examination of Digital Evidence: A Guide for Law Enforcement; U.S. Department of Justice; Office of Justice Programs. file:///C:/Users/user/Documents/FORC/resources/US-digital-forensics.pdf

PSD; the Jordanian Public Security Department; Guide for Investigating Electronic Crimes; file:///C:/Users/user/Documents/FORC/resources/%D8%AF%D9%84%D9%8A%D9%84%20%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9.pdf

PSD; the Jordanian Public Security Department; Training manual for dealing with digital evidence; file:///C:/Users/user/Documents/FORC/resources/الادلة%20الرقمية.pdf

Saeed, Kamel; the Law of Criminal Proceeding, a comparative and analytical study; (text book); Dar Al-Thaqafa; 2005; Amman; Jordan.

Chapter 3 Admissibility and credibility of evidence in digital issues

Section Number 3

Section Title **Conclusion: Admissible and credible evidence before the court**

Introduction

Content This chapter presented the concept of evidence as a method by which a fact is proved before courts; what makes good evidence, and who has the power to investigate such evidence.
As presented in previous sections, a piece of evidence must fulfill many conditions to be admissible in courts, and for the judges to rely on it. Evidence should be collected by the competent authorities, within their jurisdiction and according to the governing laws, relevant to the case at hand, compatible to the relevant formalities, properly extracted, examined and preserved, adequately documented, and comprehensible by competent courts.

Table of contents

Section Number 3

Section Title **Admissibility and credibility of evidence in digital issues**

Content

4.3 The Unit for Combating Electronic Crimes
Investigating Digital Crimes
1. Investigating stages
2. Formalities of the technical report
3. Extraction of digital evidence
4. The process of and the tools for extracting and documenting digital evidence
4.1 Tools
4.2 Steps
4.3 Documentation (chain of custody)
5. Ethics
Conclusion

Activity Number	1
Title	Challenges facing investigating digital crimes and the best approach thereto
Type	Reflection
Aim	The aim of this activity is to better understand the concept and importance of evidence (presented in sub-sections: Legal evidence in General, and: Investigating digital crimes), by reflecting on the challenges to investigating such evidence and suggesting solutions thereto.
Description	Watch the following video and then reflect on the major challenges facing investigating digital crimes, list them according to importance, then suggest the best solution to the first five. https://youtu.be/-MXgMXy7_Y4
Timeline	1.5 hrs
Assessment	- Students can do this activity either individually or via group work. - Students shall prepare a set of challenges. - Students shall discuss them in an interactive session, to come out with a set of challenges sorted according to their importance. - Students shall either evaluate each other's answer, or conduct a self-evaluation.

Activity Number	2
Title	How to provide a good chain of custody for evidence?
Type	Research
Aim	The aim of this activity is to grasp the main principles of what constitute admissible and credible evidence. Describe the aim of the activity and link the activity with a learning outcome.
Description	Write a short paper (one page) on the best approach to the chain of custody
Timeline	Take home exam (2 to 4 hrs)
Assessment	Each paper will be assessed compared to the chain provided in the subsection titled: Investigating digital crimes.

Think (MCQs) chapter 3 Admissibility and credibility of evidence in digital issues

Number 1

Title Subsection: Investigating Authorities

Type Multiple choice question

Question The persons having the authority to investigate digital crimes are:

Answers a. Judicial officers.
b. Public prosecutors.
c. The presiding judge.
d. **All of the above.**

Think (MCQs) Chapter 3 Admissibility and credibility of evidence in digital issues

Number 2

Title Subsection: Legal Evidence in General

Type Multiple choice question

Question The relevance of evidence means:

Answers a. **The facts to be proved must be productive, specific and concise.**
b. The facts to be proved must be of a digital nature.
c. All of the above.
d. None of the above.

Think (MCQs) Chapter 3 Admissibility and credibility of evidence in digital issues

Number	3
Title	Subsection: Legal Evidence in General
Type	Multiple choice question
Question	Evidence brought to court does not need to prove:
Answers	a. The three elements of the crime at hand. b. **The perpetrator.** c. Connecting the perpetrator (if known) to the crime. d. None of the above.

Think (MCQs) Chapter 3 Admissibility and credibility of evidence in digital issues

Number 4

Title Subsection: Investigating authorities

Type Multiple choice question

Question The Unit for Combating Cybercrimes is:

Answers a. Part of the Judicial authorities.

b. **Part of the Executive authority.**

c. Part of the Legislative authority.

d. Is an independent body not related to any other authority.

Think (MCQs) Chapter 3 Admissibility and credibility of evidence in digital issues

Number 5

Title Subsection: Legal Evidence in General

Type Multiple choice question

Question What from the following is not considered evidence in criminal cases

Answers a. Testimony.
b. Expert opinion.
c. The technical report.
d. **Oath.**

Extra: Chapter 3 Admissibility and credibility of evidence in digital issues

Number 1

Title Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence

Topic Subsection: Legal evidence in general

Type Maghaireh, Alaeldin Mansour Safauq; Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence; University of Wollongong; 2009. https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4404&context=theses

Extra: Chapter 3 Admissibility and credibility of evidence in digital issues
Number 2
Title Forensic Examination of Digital Evidence: A Guide for Law Enforcement
Topic Subsection: Investigating authorities
Subsection: Investigating digital crimes
Type National Institute of Justice; Forensic Examination of Digital Evidence: A Guide for Law Enforcement; U.S. Department of Justice; Office of Justice Programs.
file:///C:/Users/user/Documents/FORC/resources/US-digital-forensics.pdf

Extra: Chapter 3 Admissibility and credibility of evidence in digital issues
Number 3
Title Digital forensics and crime
Topic Subsections: Investigating authorities
Subsection: investigating digital crimes
Type Digital forensics and crime; The Parliamentary Office of Science and Technology, London; 2016.
file:///C:/Users/user/Documents/FORC/resources/uk-report.pdf

4. Overview of regulations and legislation in the different legal systems

Scope

Number 4

Title **Overview of regulations and legislation in the different legal systems**

Introduction This chapter provides a general overview of the International agreements and efforts in combating cybercrime, a general analysis of the key features in the agreements, an overview of the Budapest Convention on Cybercrime and an outline of the limitations of its application, and finally this chapter highlights the main aspects on national law in compliance with international law

Outcomes Upon the completion of this chapter, students will be able to:
1. Understand the difference between cyber security and cyber law.
2. Understand and evaluate the Budapest Convention on cybercrime (2001)
3. Analyze national law in compliance with international agreements and treaties.

Topics

National and international digital laws

International agreements

1. The Budapest Convention on Cybercrime
2. International Efforts in Combating Cybercrime
(1) Resolution 55/63
(2) Resolution 56/121
(3) Resolution 57/239
(4) Resolution 58/199
(5) Resolution 61/211

International, Regional and National Legal Agreements

1. Key Differences in the Agreements
2. Implementation of International and Regional Agreements on a National Level
3. National Law: The Jordanian Law

Study Guide

Task	Time
Preparation (Introduction and On-line Planning):	1.5 hrs
Textbook Content:	4 hrs
Thinking (online discussion review questions)	1.5 hrs
Tutorial Work on Law and Legal Systems	1.5 hrs
Related Course Work	1.5 hrs
Total	10 hrs

Required external resources:

Beebe, N.L. and J.G. Clark, 2005. A hierarchical, objectives-based framework for the digital investigations process. Digital Invest., 2: 147-167.

1

Content: Chapter 4 Overview of regulations and legislation in the different legal systems

Section Number 4

Author Mahasen Aljaghoub,
Professor of Public Law, School of Law, University of Jordan

Section Title **Overview of regulations and legislation in the different legal systems**

Introduction This Chapter tackles international and national legal instruments that regulate the matter of cyber-security.
International treaties and efforts will be outlined thoroughly. In addition to a comparative analysis of national laws in comparison with the international law is discussed.

Content The world has witnessed a great revolution in technology in the past century. As the dependence on the internet increases daily, most interactions today, whether local or international are governed by technology. Accordingly, the need for secure and trusted platforms has risen resulting in the need of a domestic and international development of cyber-security.
"The internet has brought with it a fundamental change in the way nations and their citizens engage in global economic activity, manage critical infrastructure, and communicate with one another. The hyper-connectivity of the modern world brings a wealth of benefits for governments, enterprises and individuals in that the information exchange is no longer dependent on physical constraints and is available immediately regardless of the distance (Appazov, 2014, p. 6).
In order to protect these interactions, the concept of cyber-security has risen. Cyber-security can be defined as the method used to protect computers and software from cyber-attacks. Cyber-security was also defined by the ISO/IEC 27032:2012 Information technology, Security techniques, Guidelines for cyber-security as; "preservation of confidentiality, integrity and availability of information in the Cyberspace (ISO/IEC 27032:2012).

National and international digital laws
It must be noted that "legal measures play a key role in the prevention and combating of cybercrime. Law is a dynamic tool that enables the state to respond to new societal and security challenges, such as the appropriate balance between privacy and crime control, or the extent of liability of corporations that provide services. In addition to national laws, at the international level, the law of nations – international law – covers relations between states in all their myriad forms. Provisions in both national laws and international law are relevant to cybercrime (UNDOC, 2013).

List of additional material

Section Number **4**

Section Title **Overview of regulations and legislation in the different legal systems**

Content
Appazov, Artur, Legal Aspects of Cyber-security, Faculty of Law University of Copenhagen, 2014.
ISO/IEC 27032:2012; Guidelines for cyber-security.
UNDOC, Comprehensive Study on Cybercrime, Vienna, February 2013.

Content

Section Number 4 (Overview of regulations and legislation in the different legal systems)

Section Title **International agreements**

Introduction This Chapter tackles international agreements in regard to cyber-security.

Content It should be noted that the International Law Commission adopted at its forty-eight session in 1996 The Draft Code of Crimes against Peace and Security of Mankind, and submitted it to the United Nations General Assembly. Crimes against the peace and security of mankind were then established as crimes under international law, whether or not they were punishable for binding Parties under national law. Crimes against

peace and security in cyberspace should be established as crimes under international law through a Convention or Protocol at the United Nations level (Schjolberg, 2011). Unfortunately, to date, there is no international convention or treaty drafted by the United Nations in respect of cybercrimes that is binding to all States.
On the other hand, the Council of Europe has enacted the Budapest Convention on Cybercrime which is open to all states for ratification. The Budapest Convention in addition to other resolutions adopted by the United Nation General Assembly will be discussed in further detail. Moreover, the Jordanian Cyber Crimes Law No. (27) Of 2015 will be addressed thoroughly.

1. **The Budapest Convention on Cybercrime**

The need for protecting the cyber space has risen from the very begging of its existence, "several Western nations have come together in an attempt to deter hackers and limit cyber-attacks. The Council of Europe along with the U.S. Department of Justice have been actively meeting since 1997 in the drafting of an international treaty whereby signatory countries are required to create andstrengthen their domestic laws"(Baron , 2002, p.264).
After years of extensive discussions, the Budapest Convention on Cybercrime was adopted by the Council of Europe in Budapest on November 23rd, 2001 and entered into force July 1st, 2004 (the "Convention"). Up to this day 63 countries have signed and ratified the convention and only 3 of which did not follow their signature with ratification (Council of Europe, Conventions, retrieved July 2019). The Budapest Convention is considered the only binding international treaty to address cybercrime and cyber security as it is open for ratification by states which are not members of the Council of Europe. The Convention was followed by an Additional Protocol which was adopted on November 7th, 2002 and entered into force on March 1st, 2006 (Shalini, 2016).
It is important to note that, the ratification of the international convention alone is not considered enough to combat cybercrime and enhance cyber-security. Accordingly, States must use the provisions of the Convention as guidelines and baseline to develop national legislations in compliance with the principles of the Convention.
The Budapest Convention which has been in place for more than 15 years, which has been considered as a global legal framework for cooperation has proven to be reasonably effective in creating more synergies between its signatories. It has been stated that, the state parties have harmonized their domestic laws accordingly and non-state parties have been using it as a model for their cybercrime legislation. (Hakmeh, 2017).
"The Convention contains 48 articles, categorized under lengthy chapters, tides and subsections. Its beginning starts with a preamble stating the document's intent. The intent is to foster a common criminal policy aimed at the protection of society against cyber-crime."(Baron, 2002, p. 268). The Convention essentially addresses the acts that fall within the scope of a criminal offence, the duties of each state to implement a national legislative base to incriminate such acts and finally it stresses on the importance of international cooperation in combating cybercrime and enhancing cyber-security. The second chapter of the Convention addresses the national measures that must be taken by each state and the third chapter addressed the international cooperation between states.
The Convention broadly attempts to cover crimes of illegal access, interference and interception of data and system networks, and the criminal misuse of devices. Additionally, offences perpetrated by means of computer systems such as computer-related fraud, production, distribution and transmission of child pornography and copyright offences are addressed by provisions of the Convention. The substantive offences under the Convention can broadly be classified into:
1- "Offences against the confidentiality, integrity and availability of computer data and systems;
2- Computer-related offences;
3- Content-related offences; and

4- Criminal copyright infringement."(Shalini S, 2016).
It should be noted that the first section of the second chapter of the Convention in articles 2 through 10 addresses the following offences and demands that each state implements a national legislation to incriminate it; illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to infringements of copyright and related rights.
Moreover, in Article 11, the convention addresses the liability arising from attempting to commit an offence or otherwise aiding or abetting an offence and further provides measures to be taken in this respect.
The Convention, also, in Article 12, tackles corporate liability of legal persons whereby legislative and other measures must be adopted by the parties to the Convention to ensure that legal persons can be held liable for a criminal offence established in accordance with the Convention which is committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
(i) a power of representation of the legal person;
(ii) an authority to take decisions on behalf of the legal person;
(iii) an authority to exercise control within the legal person. Subject to the local laws of parties to the Convention, the liability of a legal person may be criminal, civil or administrative, noting that such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.
It could be argued here, that according to Article (13) of the Convention, each state is to take the necessary measures to impose proper sanctions. Section two of the second chapter addressed the procedural law to be implemented by each state domestically. Moreover, the Convention, in its third chapter, thoroughly explained the means for international cooperation between the parties to the Convention, which means include: mutual assistance regarding accessing of stored computer data, mutual assistance in the real-time collection of traffic data, procedures pertaining to mutual assistance requests in the absence of applicable international agreements and extradition.
To conclude, the Convention on Cybercrime is the only binding multilateral convention to target cybercrime and cyber-security up to date.
However, considering the fact that it is issued by the Council of Europe and not the United Nations, the number of member states is relatively limited and a need for a convention that is executed or ratified by more countries, hence having a larger scope, still stands, as the cybercrime and cyber-security issue is of utmost importance today as it is relates to around 3 billion people.
In addition, it was argued that since the convention is based on criminal cyber conducts in the late 1990s, therefore, new methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, spam, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber-attacks against information infrastructures. Accordingly, some states have adopted or preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a 1990s, is not necessarily suitable for now (Schjolberg, 2011) which, indeed, further emphasizes the need for a true international treaty to address the on growing aspects of cybercrimes and cyber-security.

2. **International Efforts in Combating Cybercrime**

It is important to note that, the importance of criminalizing cyber- attacks lies in the fact that "cybercrime is quick to occur and difficult to prosecute. Network intrusions and "hacks" can take place in a matter of seconds with complete anonymity," (Baron, 2002, p. 263) threatening regular users, businesses and even countries. Therefore, it is of extreme importance to limit such attacks as the damage of cybercrime has exceeded 15 billion dollars yearly (Baron, 2002, p. 263).
Therefore, and with the absence of a solid international law base for cyber-security and cybercrime, the need for treaties and conventions has risen, however, even with

the failure to establish a multilateral treaty; this issue was addressed regionally and internationally on more one occasion.
"Certain sectorial and regional treaties taken together provide a 'patchwork of regulations' for cyber activities. These include, in particular: the 1992 Constitution of the International Telecommunication Union, the 2001 Budapest Convention on Cybercrime and its 2006 Protocol on Xenophobia and Racism, the 2009 Shanghai Cooperation Organisation's Information Security Agreement, and the 2014 African Union's Cyber-Security Convention." (Mačák, 2016).
Such treaties, which address a limited aspect of the issue and have a limited number of members, is considered relatively low. It was argued that, despite the fact that state practice in this area is inevitably shrouded in secrecy, states have been reluctant to offer clear expressions of opinion juris on matters related to cyber-security. (Mačák, 2016).
It should be noted that, in order to further analyse the international stance on cyber-security and cybercrime a look must be taken on the resolutions issued by the United Nations.
"This issue has been addressed at the following events and conferences:
(1) The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, established under the umbrella of the First Committee of the UN General Assembly;
(2) The International Telecommunication Union; in the context of international telecommunication law;
(3) The UN Human Rights Council in the context of human rights (especially the right to privacy);
(4) The G7 Summit and particularly the 2016 IseShima Summit, and of course the NATO summit meetings."(Kono, 2017).
Moreover, it should be noted that, the United Nations General Assembly has adopted five resolutions regarding cyber-security and cybercrimes:
a. **(1) Resolution 55/63, January 2001: Combating the criminal misuse of information technologies:**
The following was concluded in this resolution:
• - "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;
• - Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;
• - Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;
• - Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;
• - Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;
• - Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;
• - Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;
• - The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;
• - To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;
• - The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse"(Resolution 55/63, 2001).

b. **(2) Resolution 56/121, January 2002: Combating the criminal misuse of information technologies:**
1. - "Invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;
2. - Takes note of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;
3. - Decides to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice."(Resolution 56/121, 2002).

c. **(3) Resolution 57/239, January 2003: Creation of a global culture of cyber-security:**
In this resolution, the United Nations General Assembly recognized and addressed the need for the enhancement of international law in the field of cyber-security and cybercrime, and noted that "the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information," (Resolution 57/239, 2003), therefore, it referred to its previous relations and asked the member stated to take measures to implement its previous recommendations. In addition, the resolution stressed on the need of awareness as it was mentioned that "in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cyber-security risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies." (Resolution 57/239, 2003). Finally, it further stressed the need for international cooperation in the matter.

d. **(4) Resolution 58/199, January 2004: Creation of a global culture of cyber-security and the protection of critical information infrastructures:**
In this resolution, the General Assembly has Stressed the necessity for enhanced efforts to close the digital divide and to achieve universal access to information and communication technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building. (Resolution 58/199, 2004)

e. **(5) Resolution 64/211, March 2010:Creation of a global culture of cyber-security and taking stock of national efforts to protect critical information infrastructures:**
This resolution aimed to discuss the need of the implementation of national measures in the issue and the resolution reaffirmed "the continuing need to enhance cooperation, to enable Governments, on an equal footing, to carry out their roles and responsibilities ininternational public policy issues pertaining to the Internet, but not the day-to-day technical and operational matters that do not impact on international public policy issues" (Resolution 64/211, 2010), and further stressed "the need for enhanced efforts to close the digital divide in order to achieve universal access to information and communications technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building to developing countries, especially the leastdeveloped countries, in the areas of cyber-security best practices and training."
As a conclusion, the United Nations General Assembly addressed the issue on five separate occasions four of which were resolved in consecutive years, noting that the last resolution has been issued eight years ago. However, the resolutions are not considered binding and therefore the need for an international treaty drafted by the United Nations remains.

List of additional material

Section Number	**4 (Overview of regulations and legislation in the different legal systems)**
Section Title	**International Agreements**
Content	Baron, Rayan M.F., A Critique of the International Cybercrime Treaty, Commlaw Conspectus, Vol. 10, 2002. COE, Council of Europe, Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, 2019: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Last visited July 2019. Hakmeh, Joyce, Building a Stronger International Legal Framework on Cybercrime, Chatham House The Royal Institute Of International Affairs, 6 June 2017. Kono, Keiko, International Laws on Cyberattacks that Do Not Constitute an Armed Attack, October 2017 Edition. Mačák, Kubo, Is the International Law of Cyber Security in Crisis, University of Exeter, Exeter, United Kingdom, 8th International Conference on Cyber Conflict, N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.) 2016 © NATO CCD COE Publications, Tallinn. Resolution 55/63, January 2001: Combating the criminal misuse of information technologies Resolution 56/121, January 2002: Combating the criminal misuse of information technologies Resolution 57/239, January 2003: Creation of a global culture of cyber-security Resolution 64/211, March 2010: Creation of a global culture of cyber-security and taking stock of national efforts to protect critical information infrastructures Resolution 64/211, March 2010: Creation of a global culture of cyber-security and taking stock of national efforts to protect critical information infrastructures Schjolberg, Stein and Ghernaouti-Helie, Solange, A Global Treaty on Cyber-security and Cybercrime, 2011. Shalini S, Budapest Convention on Cybercrime, Information Law and Policy Research at the Centre for Communication Governance, March 3, 2016.

Content Section Number	4 (**Overview of regulations and legislation in the different legal systems)**
Section Title	**International, Regional and National Legal Agreements**
Introduction	This Chapter tackles international, regional, and national legal agreements of cyber-security.
Content	"The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. The genesis, legal status, geographic scope, substantive focus, and mechanisms of such instruments vary significantly (UNDOC, 2013). The below table identifies the legal instrument, whether it is binding or not in addition to its source and year of issue.

Binding	Non-binding
▪ Council of Europe Convention on Cybercrime (2001) and Additional Protocol (2003) ▪ Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007) ▪ EU legislation including on e-Commerce (2000/31/EC), on Combating Fraud and Counterfeiting of Non-Cash Means of Payment (2001/413/JHA), on Personal Data (2002/58/EC as amended), on Attacks against Information Systems (2005/222/JHA and Proposal COM(2010) 517 final), and on Child Pornography (2011/92/EU)	▪ Commonwealth Model Laws on Computer and Computer-related Crime (2002) and Electronic Evidence (2002)
▪ Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001) ▪ Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009)	
▪ (Draft) Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime (2009) ▪ (Draft) African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012)	▪ East African Community Draft Legal Framework for Cyberlaws (2008) ▪ Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Draft Model Bill (2011) ▪ Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2012)
▪ League of Arab States Convention on Combating Information Technology Offences (2010)	▪ League of Arab States Model Law on Combating Information Technology Offences (2004)
▪ Optional Protocol to the United Nations Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000)	▪ International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU) Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010) ▪ International Telecommunication Union (ITU)/Secretariat of the Pacific Community Model Law on Cybercrime (2011)

Table (1): A summary of binding and non-binding legal instruments
*Source: UNDOC, 2013.

Indeed, not all previously mentioned instruments are identical, notable differences can be seen in each one; however, all are similar in their essence.

1. **Key Differences in the Agreements**

Indeed, not all agreements are identical, they differ according to the region or the country that developed the agreement; however, all agreements are aligned with the main principles that govern the matter.
Below is a table that highlights the key differences and similarities in the agreements.

Criminalization	• Most instruments contain an extensive list of offences. Others focus only on a limited thematic offence area, such as instruments focusing on child pornography and child protection • Acts against the confidentiality, integrity and availability of computer data or systems are most commonly criminalized, followed by computer-related fraud or forgery, and computer-related production, distribution or possession of child pornography • Some instruments provide that conventional crimes committed by means of a computer system should be an aggravating circumstance
ProceduralPowers	• Search, seizure, orders for stored computer data and subscriber information, real-time collection of computer data, and expedited preservation of computer data are themost common procedural powers • Trans-border access to computer data is envisaged by three instruments
ElectronicEvidence	• The few (mainly, non-binding) instruments that address electronic evidence cover areas including the general admissibility of electronic evidence, the burden

	of proving authenticity, the best evidence rule, the presumption of integrity, and preservation standards.
Jurisdiction	• Nearly all instruments include the territorial principle and nationality principle (where dual criminality exists) as bases for jurisdiction • Other bases for jurisdiction, not found in all instruments, include acts directed against a computer system or data located within the territory and a state interests' principle • Two instruments provide guidance on establishment of the place of a cybercrime offence.
InternationalCooperation	• Instruments tend to either address international cooperation extensively – providing mechanisms for mutual legal assistance and extradition – or to focus in a more limited way on general principles of cooperation • A number of instruments envisage the establishment of points of contact or 24/7 networks
Service Providers	• The limited number of instruments that address the responsibility of service providers cover areas including monitoring obligations, voluntary supply of information, take-down notifications, and liability of access, caching, hosting and hyperlink providers

Table (2): the key differences and similarities in cybercrimes agreements
* Source: UNDOC, 2013.

2. **Implementation of International and Regional Agreements on a National Level**

It is important to note that the way in which international or regional agreements are implemented in national law is different in each member state. States may interpret or implement the provisions ofinternational agreements in different ways, leading to further divergence across countries (UNDOC, 2013).

In conclusion, each country or member state must provide provisions that comply with the agreement in its national law. However, the provisions of the agreement may seem different in each country and that is because the manner of implementation differs according to various numbers of factors that govern the national law.

Accordingly, the effectiveness of the national law varies from country to country. Yet as previously explained, all laws meet the terms of the international and regional agreements.

3. **National Law: The Jordanian Law**

It should be noted that there are seven categories of cybercrimes have been stipulated under the Jordanian cyber law of 2015 which is discussed thoroughly in the first and second chapters.

List of additional material

Section Number	**4 (Overview of regulations and legislation in the different legal systems)**
Section Title	**International, Regional and National Legal Agreements**
Content	UNDOC, Comprehensive Study on Cybercrime, Vienna, February 2013. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

Activity Number	4.1
Title	Analysis of the Budapest Convention in compliance with the National Law
Type	Reflection
Aim	The aim of this activity is to better understand and analyze the Budapest Convention on cybercrimes (presented in sub-sections: international agreements) and also to understand how member states of the convention can develop national legislations to provide a legal framework for international cooperation among countries (presented in sub-section: international agreements and implementation of international and regional agreements on national level) .
Description	Read and analyze the Budapest convention, then reflect on the major challenging facing member states in complying with the convention. List them according to importance, then determine whether your country is a member state of the Convention; if so, to what extent does the national law (governing the matter) in your country comply with the provisions of the Convention. Otherwise, write a short paper (one page) to highlight the main reasons that might have prevented your country from joining the Convention in your opinion; and what are the key features in the national law that might be similar to the Convention.
Timeline	Time: 1 hour
Assessment	- Students can do this activity either individually or via group work. - Each Student must provide provisions that comply with the convention on his/her own national law, or, otherwise should prepare a set of challenges that might have prevented his or her country from joining the convention. - Students should discuss their work in an interactive session to come outwith a set of challenges sorted according to their importance preventing states from complying with the convention. - Students should either evaluate each other's work or conduct a self-evaluation.
Scenario	
Reference	The Budapest Convention on Cybercrime, ETS 185 – Convention on Cybercrime, United Nations Resolutions provided in the chapter Students' National laws related to Budapest Convention

Think (True or False) Section 4 Overview of regulations and legislation in the different legal systems

Number 1

Title International Efforts in Combating Cybercrime

Type True or False

Question Is there a precise definition for cybercrime that is agreed upon in the international law?

Answers **Answer: False**

Think (True or False) Section 4 Overview of regulations and legislation in the different legal systems

Number	2
Title	**International agreements**
Type	**True or False**
Question	Did International efforts succeed in combating cybercrimes?
Answers	**Answer: False**

Think (True or False) Section 4 Overview of regulations and legislation in the different legal systems

Number 3

Title **International, Regional and National Legal Agreements**

Type **True or False**

Question Is There a treaty for the Arab region to combat cybercrimes

Answers **Answer: True**

Think (True or False) Section 4 Overview of regulations and legislation in the different legal systems

Number 4

Title **International, Regional and National Legal Agreements**

Type **True or False**

Question Is there a specialized court that prosecutes the crimes committed in cyber space in your country?

Answers **Answer:**

The answer depends on each students' state

In Jordan and Palestine, the answer is: False

Extra: Chapter 4 Overview of regulations and legislation in the different legal systems
Number 1
Title **Guidelines for cybersecurity**
Topic **Overview of regulations and legislation in the different legal systems**
Type ISO/IEC 27032:2012; Guidelines for cybersecurity.

Extra: Chapter 4 Overview of regulations and legislation in the different legal systems
Number 2
Title **The UN Resolutions on cyber security and cybercrimes:**
Topic **International agreements**
Type 1. Resolution 55/63, January 2001: Combating the criminal misuse of information technologies
2. Resolution 56/121, January 2002: Combating the criminal misuse of information technologies
3. Resolution 57/239, January 2003: Creation of a global culture of cyber-security.
4. Resolution 58/199, January 2004: Creation of a global culture of cyber-security and the protection of critical information infrastructures.
5. Resolution 64/211, March 2010: Creation of a global culture of cyber-security and taking stock of national efforts to protect critical information infrastructures

Extra: Chapter 4 Overview of regulations and legislation in the different legal systems
Number 3
Title **UNDOC, Comprehensive study on Cybercrime**
Topic International, Regional, and National Legal Agreements
Type UNDOC, Comprehensive Study on Cybercrime, United Nations Office On Drugs and Crime, Vienna, February 2013.