Journal of Politics and Law; Vol. 7, No. 2; 2014
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Cyber Crimes and Technical Issues under the Jordanian Information System Crimes Law

Raed S A Faqir[1], Saleh Sharari[2] & Salameh A. Salameh[3]

[1] Zarqa University College, Balqa Applied University, Jordan

[2] Al. Hessian University, Jordan

[3] Balqa Applied University, Jordan

Correspondence: Raed S A Faqir, Zarqa University College, Balqa Applied University, Jordan. Tel: 9-627-7767-3608. E-mail: fageerjo@yahoo.com

Received: July 26, 2013 Accepted: August 30, 2013 Online Published: May 28, 2014

doi:10.5539/jpl.v7n2p94 URL: http://dx.doi.org/10.5539/jpl.v7n2p94

Abstract

The Information Systems Crimes Law No (30) of 2010 has been dealt in detail and other traditional criminal laws were discussed in brief. The primary objective of the current study was to determine the Jordanian legal mechanism for fighting cyber-crimes with concentrating on Information System Crimes Law, 2010, cyber-crime's terminology, nature and scope, and challenges to criminal justice system in Jordan. The second objective was to determine and analyze Jordanian criminal statutes of cyber-crimes, cyber-criminal activity, cyber-crimes against Persons, and cyber-crimes against property, criminalities and technology. A final objective was to identify impact of cyber crimes on criminal law, limitations of Jordanian cyber- crimes law of 2010.

Keywords: cyber-crimes, Jordan, legal system, ISC Act, Botnets, Phatbot, DDoS, IRC, WASTE

1. Introduction

In today's globe, the threat of cyber-crimes has affected all the levels of life, it breaches security of communities by targeting both individuals and organization with smart techniques and all counter tech-tools, as "perimeter-intrusion detection, signature-based malware, and anti-virus solutions" are not sufficient for compacting this type of crimes (Deloitte, 2010). The new generation of crimes as the result of the enormous developments in the digital globe differs somewhat from conventional offences. In cyber-crimes the criminal does not carry a revolver or burgles the mall market, but while having full privacy at home and by using his or her computer or laptop through Internet starts with commission of the crime and the victim will at any corner of the world.The major serious threats of crimes committed cyberspace, as outcomes of the growth of information society that are affecting the essential services such as "water and electricity supply now rely on ICTs, cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs", and more complicated cyber-crimes has revealed such as "attacks against information infrastructure and Internet services, Online fraud and hacking attacks" (Gercke, 2012). As cyberspace offenders persist to generate and extend their techniques, they are also changing their aims by concentrating on business espionage and unauthorized accessing of both individual and governmental information. Hence, the legal, technical challenges of cyber crimes have increased, which means no country can solely fight fast-spreading cyber offences, where there is a need for each country to collaborate globally to develop its legal and technical mechanism for controlling such a threat (KPMG International, 2011).

As is always the case, national legislations takes into account the development of technology and its use by the criminals who continue to develop their techniques in order to carry out their criminal activities smoothly. The Electronic Transactions Act No (85), 2001 is deemed as the first law in Jordan that designed for the investigation and prosecution of cyber-crimes and computer- related crimes, but the major concentration of its provisions was on the electronic transactions from commercial angle and criminal prospective. The problem of the Jordanian traditional criminal laws in dealing with cyber-crimes is apparent, such laws were designed in the last century for the purpose of combating conventional crimes, and specifically those laws were designed at the time before the emergence of digital era in area as well as those law were translated from its historical French source on the time of Outman Empire with no significant amendment (Faqir, 2004).

2. Problem of the Study

The Phenomena of high-technology offences, including electronic, internet, cyber, crimes and computer related crimes, is new and has serious impacts on the contemporary societies due to the size of loess resulted from (Arab, 2002). Cyber crimes and computer enabled crimes have different characteristics in comparing with traditional crimes, and even there is a variety between physical space of criminal law traditional crimes and cyberspace of high-technology crimes including cyber-crimes (Hawkins, 2001). The main dissimilarities between virtual cyber-crimes and traditional offences are the object, venue as well as anonyms, while cyber crimes target data and information within cyberspace and committed in anonyms way, the traditional crimes target either property or persons within the physical world and there is always a physical scene for the committed crimes (Dunn, 2007; Finklea, 2012; Mitchell, 1995; Barry, 2012; Kenneth, 2011).

Jordan is not isolated from its global environment; it suffers from the negative impact of cyber-crimes and faces lot of challenges in dealing with the new type of cyberspace crimes. At the beginning, prior to the enactment of new Information Systems Crimes Law No (30) of 2010, there were many attempts to apply the paradigms of the traditional criminal theory contented in the Punishment Code of Jordan, 1960 but all of these attempts failed.

Cyber offences are considered as complicated issues for police force and judicial police in Jordan because they are new and unique crimes that differ from traditional ones. Police officers need to be trained in cyberspace technology and forensics in order to investigate and prosecute ant type of computer- enabled crimes. Additionally, the Cyber Crimes law, 2010 and other Cyber and Criminal Laws in Jordan have to be updated and amended in order to criminalize all the potential cyber crimes with outlining appropriate penalties for those crimes. The negative impact of cyber crimes can't be mitigated unless the agents of the criminal justice system of Jordan are well equipped and knowledgeable about last continuing computer- related technologies and techniques.

Recognizing the vital obstacles and problems emanating from cyber-crimes, the current study is trying to explain the legislative defects in the Cyber Crimes Law of Jordan, 2010 and the problems faced by public authorities in dealing with those crime because the absence of legal foundation for investigating and prosecuting cyber-criminal activities within the context of Jordanian criminal justice system. Specifically, the study focus on: the definitions of cyber-crime, nature & scope of computer-related offenses, challenges to criminal justice system in Jordan, criminal statutes of cyber-crimes, cyber-criminal activity, cyber-crimes against Persons, cyber-crimes against property, criminalities and technology, effect of cyber offences to traditional legislation, limitations of Jordanian cyber- crimes law, 2010.

3. Hypothesis of the Study

The current study is about "the law relating Cyber Crimes in Jordan with special reference to Information System Crimes Law No (30) of 2010". The first hypothesis to be tested in this study is that there is a relationship between increasing cyber crimes in Jordan and legislative defects in the cyber- laws, the study shows that the absence of legal foundation in the field of cyber crimes poses more challenges on criminal justice agencies for investigating and prosecuting those types of crimes. The literature review of the studies revealed that the main traditional criminal laws might be incompatible for cyber crimes and special cyber laws are needed for these unique crimes. The second hypothesis of this study is the legal and technical challenges caused by cyber crimes linked with the existence of inefficient criminal and cyber laws.

4. Importance and Objectives of the Study

The primary objective of the current study was to verify the efficiency of legal instrument in Jordan for fighting cyber-crime by focusing on the provisions of Information System Crimes Law, 2010, cyber-crime's terminology, nature and scope, and challenges to criminal justice system in Jordan. The second objective was to analyze Jordanian criminal legislation of cyber-crimes, cyber-criminal activity, cyber-crimes against Persons, and cyber-crimes against property, criminalities and technology. A final objective was to identify impact of cyber crimes on criminal law, limitations of Jordanian cyber- crimes law of 2010.

5. Methodology of the Study

The present study is an exploratory one and hence a multipronged methodology is used to complete the study. This is included analytical and descriptive method as far as historical development and analysis of legal framework is concerned. The analysis of impact of cyber crimes and the legal mechanism for compacting it in Jordan based on data that gathered through published annual Reports, Articles published in books, journals and newspapers etc. Electronic articles, books and materials posted on Internet websites are consulted. Thus, both primary and secondary sources are made use of in the completion of study. The sections of Jordanian

Information Systems Crimes Law of 2010, Criminal Procedural Code, 1961, Punishment Code of 1960 and Sections of other related legislations and laws in Jordan are already reviewed.

6. Challenges to Criminal Justice System in Jordan

Cyber-crimes represent a real challenge to all criminal justice systems all over the world including Jordan, as the matter of differences between cyber and conventional crimes discussed previously, it is seen that cyber-crimes are distinguished from traditional crimes because of its target, venue and anonymity. On this basis, such sort of crimes are unique in each and every sides of its elements, in some way requires from the police and prosecution authorities to be more vigilant, specialized and accurate in dealing with it.

In present days, the computer's modern techniques become essential for all types of transactions and activities carried out by human beings within every aspect of their life., where fax, automated calls, mobile phones, imaging scans, medical equipments, surgical operations, e-commerce, elevators, e-transport and space communications, ATM cards, e-commerce, e- economy, control of the military machine and weapons of mass destruction are operated and controlled by technologies of computer. The use of Global Information Infrastructure contributes vitally in the increment of the size and number of committed cyber-crimes all over the world, where Jordan is not isolated from. The repaid technological advancements of space related techniques, security and political instability and diversification of cyber offences in most of countries generate some sort of complexity in controlling these crimes by public authorities, and make the criminal justice system and its different agencies very weak in combating such crimes.

Criminal justice system of any country is a real mirror for the degree of urbanization and civilization of society, as well as the observer for each negative behavior of its members. The shortage in the provisions of the Information Systems Crimes Law No (30) of 2010 (Cyber-crimes Law) might be referred to the lake of knowledge of Jordanian legislators about the real developments in network technology and the delay response to the speed developments in techniques of cyberspace. The present law is not suitable to be considered as the foundation for investigation and prosecution of cyber-crimes, because it has not covered the major cyber-criminal activities, as well as the absence of procedural solution for investigation and prosecution of this type of crimes. It is observed that the provisions of Cyber Crimes of Jordan, 2010 don't provide sufficient coverage against several crimes committed in cyberspace, especially the computer-related crimes of aiding and incite hi-crimes, cyber-crimes, and computer-enabled offences of forgery and fraud.

In this regard, criminal laws in Jordan should be reviewed in order to combat cyber crimes, especially offences that have been criminalized under Jordanian Punishment Code, 1960 need to be entirely revised as to include the new generations of crimes committed in cyberspace. The digital evidences in the field of criminal cases to be treated in equivalent status of traditional and physical evidence for proving criminal cases, thus present Cyber Crimes Law in Jordan has no specific legal mechanism for combating and prosecuting cyber crimes on the light of absence of integration cyber-related crimes.

The main challenges of the legal system of Jordan is the delay in reviewing and amending criminal legislations as the speed development of technologies resulted always in bringing up new types of offences, especially in the field of new generated crimes of hi-technology, such as cyber-crimes. Hence, any future attempt to amend the Cyber Crimes Law, the Punishment Code or Criminal Procedural Code need to be made in cooperation with other countries and international society to avoid the problem of duplication and loss of resources, the experience of other countries in fighting cyber-crimes should be considered, especially with fast and speed developments of technology.

7. Criminal Statutes of Cyber-crimes

Jordan has enacted Electronic Transactions Act No (85), 2001. This law aims to facilitate the use of electronic means in order to conduct transactions, taking into account the provisions of any other laws, without making amendments or cancellations to any of these provisions and the application of these provisions should be in parallel with the International customary rules related with e-transactions and its technology exchange.The scope of this law is electronic transactions, records, signatures and any electronic information message irrespective whether these transactions are approved by any government department or official institutions[1]. Therefore, it can be observed that the Jordanian Electronic Transactions Act No (85), 2001 does not deal with cyber-crimes in

[1]. Section 4 of the Information SystemsCrimes ActNo (30)of 2010 provides that: The provisions of this Law shall apply to the following: " A- Electronic transactions, electronic records, electronic signatures and any electronic data messages. B- Electronic transactions adopted in whole or in part by any governmental department or public institutions".

direct way, even its provisions bring nothing on offensive action and design no penalties in this regard, because the legislator in that period may be was not well aware and understating the problem of computer related crimes.

The Information System Crimes Law No (30) of 2010 being the first Jordanian law on cyber-crimes, computer-enabled offences and crimes committed by use of electronic devices, this law was the production of fast governmental make up, as a temporary law made by the government it has not subjected to any type of parliamentary review or debates, therefore lot of criticisms are directed to its vague and confusable provisions. The structure of Jordanian ISC Law of 2010 is very simple, it totally has 18 sections without chapters, and it embodies two types of substantive and procedural rules. This Law begins with preliminary definitions; describe cyber crimes under sections 3 to 12 and lays down penalties therefore. The Law also is applicable within the entire territories of Jordan and except otherwise provided, the capability of ISC law, 2010 is made even in the case of crimes committed outside Jordan.

Hence, the problem of investigating and prosecuting cyber-crimes faced by the different agencies of Jordanian criminal justice system still unsolved and the traditional criminal laws in our country are paralyzed before the new technology based crimes. The Cyber Crimes Law in Jordan is insufficient in its substance, because it is being referred in the reliance and process to the Criminal Procedural Code and Punishment Code half century – old. Up to this fact, there is a real need for an amendment – a detailed one – of the 2010 Law. Before doing so all related sectors in the country should be consulted not only inside the criminal justice system, but also in the private sector itself. Legislations and experiences of other nation for investigating and prosecuting cyber crimes should be taken into account for the purpose of enactment of sufficient and effective legal frame work to the cyberspace's crimes.

8. Cyber-criminal Activity

Since decades ago cyber-crimes are considered as an artifact of computer systems, and these crimes became as a serious phenomena only with introducing the network system of computers (Alaganandam, 2005), where networking in the cyberspace differs from traditional media, like newspapers, radio, and television, because the Internet is a hybrid communication technology that could not be used only as mass communication, but also as personal communication within limited scope (El-Shehri, 2011). With Internet a progressively essential element of everyday life, perpetrators are uncovering new playing fields in cyberspace (Chen, 2010).

The criminal activity takes place in cyberspace when it is connected with a network, and especially uses the computer as target, tool or place for the committed offence. Cyber-crimes cover a broad scope of criminal activity that may include basically crimes against persons, property or government. The criminal activity in cyber-crimes takes varying forms as following:

9. Cyber-crimes against Persons

This type of crimes may include several criminal activates such as transmission of child-pornography, immoral harassments, displaying pornography and indecent exposure, cyber-homicide (Louis, 2000), extortion (Goodman, 1997) and cyber-bullying (Su & Holt, 2010). It is, however, hardly to say that the cyber-crime has any direct harm on human-body at least till this moment, but may be imaginable in future. Moreover, the cyber stalking or what is knownasonline harassment and intimidation take varying forms on the cyberspace, where it may include the sexual, racial or religious harassments (Jaishankar, 2007). The crime of child-pornography is defined as "any audiovisual material which uses children in a sexual context" (Council of Europe, 1993); such offence is classified as a cyber-crime when it is committed by using a computer or network system.

Under the Jordanian Information System Crimes Act No (30) of 2010, there many acts that recognized as cyber-crimes against persons, such as cyber-pornography[2], cyber-crime against right to privacy[3], cyber-espionage[4],

Cyber-pornography is penalized under Section 8 of the Jordanian Information System Crimes Act, which stipulates that: "Anyone who intentionally transmits or publishes through an information system or any information network anything heard [audio], read or graphic containing pornographic materials involving or relating to sexual exploitation of those who have not attained eighteen years of age". The child pornography is recognized by this Act as a cyber-crime against person whom their age does not exceed eighteen year, because

[2].Section 8 (a), (b) and (c) of the Jordanian Information Systems Crimes Act No (30) of 2010

[3].Section 3 (b) of the Jordanian Information Systems Crimes Act No (30) of 2010

[4].Section 5 of the Jordanian Information Systems Crimes Act No (30) of 2010

they are considered children and easily effected by the crime of pornography. Section 8 of the Information System Crimes Act No (30) of 2010 states also the tools by which the child pornography may be committed, these are "an information system[5] or any information network[6]", which can be used for transmitting, publishing pornographic materials. Such intentional acts are considered as illegal and punishable by paragraph (a) of Section 8 of the same Act. For example, using the Internet of any sort of pornographic transmission or publishing can lead to an imprisonment for not less than 3 months and fine of JD300 to JD5000. The legislator made the punishment for child pornography more severe in paragraph (b) of the same Section, when the act is committed against child who suffers from psychologically or mentally disabled, the punishment here is the imprisonment for not less than two years and 1000 to 5000 JD fine[7]. Moreover, It is noted here that the Jordanian legislator under section 8 (c) designs more severely punishments for the perpetrators, who commit the crime of exposing children with psychological and disabilities to prostitution or pornographic activities, they are punished more severely with the temporary penal servitude and JD 5000 to 15000 fine[8].

Cyber-crime against right to privacy is embodied implicitly in section 3 (b) ofthe Jordanian Information System Crimes Act, where the paragraphs (a) and (b) of this section stipulates that "Anyone who intentionally accesses a website or information system in any manner without authorization or in violation or excess of an authorization….. for the purpose of for the purpose of disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information". Therefore, the violation of the privacy of person on his own private data or information, either by the act of authorized or un-authorized access to the information system or network, amounts into a cyber-crime in the language of section 3 (a) and (b) of the Information System Crimes Act[9]. Under section 3 of this Act this crime is punished with a penalty of imprisonment from 3 months to one year, and JD 200 to 1000 fine[10].

Cyber-espionage is "the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward" (O'Hara, 2010: 242). The current Jordanian criminal law prohibits the act of espionage in many fields, especially in relation to banking, commercial and financial transactions, the Information System Crimes Act of 2010 prohibits cyber-espionage in section 5, which prescribes this act as "eavesdropping on what is transmitted through the Internet or any information system"[11].

10. Cyber-crimes against Property

Cyber-crimes against property is all physical offences committed by the use of computer system or network systems, and usually aim at destroying or preventing others' property. In this language the Jordanian legislator preferred to deal with all traditional crimes against property that already provided in the Jordanian Punishment Code as cyber-crimes on the basis of using the computer or network in its commission. Section 14 of the Jordanian Information Systems Crimes Act No (30) of 2010 stipulates the possibility of the application of provisions of this Act on all physical crimes against property in case of proving its commission by computer

[5].Information System can be defined as "a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose". See in general the definition of the term of " information system" at http://wiki.answers.com/Q/What_is_the_definition_of_information_system (Accessed June 20, 2012)

[6].Information Network can be defined as "a service that provides a variety of information services to subscribers on a dial-up basis, it is also known as subscription data base". See http://encyclopedia2.thefreedictionary.com/information+network (Accessed June 20, 2012)

[7].Section 8 (b) of the Jordanian Information SystemsCrimes ActNo (30)of 2010

[8].Section 8 (c) of the Jordanian Information SystemsCrimes ActNo (30)of 2010

[9].Section 3 (a) and (b) of the Jordanian Information SystemsCrimes ActNo (30)of 2010

[10].Section 3 (b) of the Jordanian Information SystemsCrimes ActNo (30)of 2010

[11]. Section 5 of the Information SystemCrimes Act of 2010 stipulates that Any person whointentionally, without obtaining permission from theAttorney General, capture orinterceptoreavesdropon what istransmitted across theInternet orany information systemis punishableby imprisonmentfor not less thanone month and notexceeding one yearor a fineof not less than(200)two hundreddinersand not more than(1000)thousanddiners, orboth penalties.

usage, such crimes as provided in the Punishment Code, 1960 are theft[12], purchasing, selling and mediation of stolen materials[13], rubbery[14], intimidation and extortion[15], unjust usage of others belongs[16], fraud[17], exploitation of minors and incapable persons[18], fraud against creditor[19], hiding information or counterfeiting certificates of the property[20], issuing a check without balance[21], and abuse of trust[22].

The outcomes of online crimes may be always same as offenses in the real realm analogues (McMullan &Rege, 2007). For instance, cyber-theft, like the traditional crime of theft, demands that the perpetrator have behaved with the motive of depriving the victim from his/her property. This condition is seen in most of the crimes of theft or steals against property, such as online commercial or financial fraud, counterfeit, extortion or blackmail etc. The culpability of cyber-crimes against property may remain the same for all other online crimes either its commission were against persons, states or morality. The criminal activity or behavior of human-beings is steady in both physical and virtual offence, and for long time ago criminal justice agencies gained good experience in understanding human misbehavior, thus there is no need change the theories of crimes entirely in the term of dealing with the crimes of new digital era.

11. Cyber Crime from Police Perspective and the Problem of Prosecution

All over the world, criminal law deal in proper way with all types of computer related offences or electronically committed offences. Cyber crimes are relatively neoteric as they originate from and in associated with the world of digital globalization, which intimidates the operation of the computer as something precious for the informatics' community.

The impact of cyber-crime on criminal law in Jordan has different legal and procedural dimensions; it generates problematic and serious impacts on both police and public prosecution efforts for prevention crimes and achieving justice. In this regard, such type of crimes still poses a threat to social security of people due to unique nature of the series of activities carried out by using computers, hi-technological and electronic devices. This new sort of "offenses" forced Jordanian criminal legislator for a comprehensive review of the provisions and rules of criminal law, this review showed that the traditional criminal laws in Jordan are paralyzed to solve the problems of these crimes, because the application of such laws requires the occurrence of these offense on material properties, while the subject of cyber crimes might be nonphysical properties not covered by these laws (Arab, 2002).

In Jordan, police faces two types of difficulties in dealing with cyber crimes, these are mainly substantive problems related to the new nature of those crimes and the inadequacy of traditional legal provisions, while the other problem is procedural, such as the difficulties of preventing and proving crimes (Afifi, 2013). Upon these problems, any medications or changes to the Jordanian Cyber Crimes Act should concentrate on the function of judicial police and justice agents in compacting cyber crimes and computer- related crimes, this task can be achieved only by vesting their powers by confining the work of net providers to the prior permission of police, which needs also police to be more involved with the global efforts in fighting cyber-ism (Afifi, 2013).

The special and unique features of the cyber-crimes and the it's hidden, confidential and anonymity nature imposes more challenges in the face of public prosecution in Jordan, the task of public prosecutor in detecting crimes and offenders very complicated. In the light of increasing of this type of crimes, there was a real need to amend the Law of on Public Prosecutor (11) of 2010, because cyber crimes investigation should be carried by central prosecutors and specialists, as provided in Section 16 of the same Law, in order to accomplish the

[12]. See Sections 399-401 of the Jordanian Punishment Code No (16), 1960.

[13]. See Sections 412 and 413, Ibid.

[14]. See Section 402, Ibid.

[15]. See Section 414, Ibid.

[16]. See Section 416, Ibid.

[17]. See Sections 417 and 418, Ibid.

[18]. See Sections 418, Ibid.

[19]. See Sections 419, Ibid.

[20]. See Sections 420, Ibid.

[21]. See Sections 421, Ibid.

[22]. See Sections 422, Ibid.

integration for control such crimes, therefore prosecutors have to be subjected to comprehensive training programs (Abu Jumaa, 2012).

Before 2010, prosecutors and judges in Jordan were entirely relied on Punishment Code, 1960 in dealing with cyber-crimes, by restoring to ordinary provisions of this law which are related to criminal activities of theft, trespass, crimes against property and criminal mischief. Moreover, the power of prosecutor to investigate such crimes were restricted to the general theory of searching and seizing by limiting access to information systems and computer's data in the same way made to physical terminals. The situation has been changed by enacting the present Information *System Crimes Law* (Cyber Crime Law)[23], which was approved on 3rd August 2010 in order to "address a legal vacuum in new digital crimes that the Jordanian criminal law could not address effectively, and to provide trust over internet networks for internet users" (Olwan, 2010).

The new law has addressed a variety of crimes that were not covered by the Punishment Code, 1960. It criminalizes several cyber related crimes, as provided in Sections 3-11 of the Information Systems Crimes Law (Cyber Crimes Law, 2010). Harsh penalties were brought up by the same Law like imprisonment punishment including hard labor and higher fine in cases of entering the information systems for "intent to copy, transfer, alert, damage, or abolish any data or information" (Al Tamimi, 2010). The Law also set up a legal infrastructure for treating different types of "credit banking scams" and made them punishable with imprisonment and fine, as well as new activities such as child pornography, sexual exploitation and online prostitutions were criminalized and made punishable by the Cyber Crimes Law, 2010 (Al Tamimi, 2010). Moreover, the Jordanian Cyber Crimes Law, 2010 paved the way before prosecutes and judges to refer to the provisions of punishment Code, 1960 in all traditional crimes that may be committed by any electronic means, such as communication offences, harassment and offences against the person.

12. Limitations of Jordanian Cyber-crimes Law, 2010

Despite Jordan's Cyber Crimes Law, 2010 criminalizes a number of electronic crimes or information, but still a lot of cyber activities are not criminalized and simply it becomes upon the prosecutor or the judge to refer to the provisions of the Jordanian Penal Code, 1960. There are many actions and activities have been criminalized by the Law, theses namely are unauthorized access to information system[24], tampering with information systems through destroying, deleting or copying it[25], impersonation[26], impeding the information system by jamming or disruption[27], or interception of information by unauthorized electronic eavesdropping[28], unlicensed obtaining information about credit cards and financial or banking transactions[29].

The law also prohibits pornography, sexual exploitation of children[30], and activities of online prostitution[31], facilitation or support of terrorist acts, promotion of terrorist ideologies[32], and having illegally access to information concerning national security or relationships with foreign countries or safety and national economy[33].

---

[23] The Jordanian Council of Ministers approved the Information Systems Crimes Law (Temporary Cyber Crimes Law) No.30 of 2010 on the 29th of August 2010, and which has come into force on the 16th of October 2010.

[24] Section 3 (a) of the Jordanian Information Systems Crimes (Cyber Crimes Law) No. 30, 2010

[25] Section 3 (b) , Ibid

[26] Section 3 (b) , Ibid

[27] Section 4, Ibid

[28] Section 5, Ibid

[29] Section 6 (a) Ibid

[30] Section 8 (a) , Ibid

[31] Section 8 (d) , Ibid

[32] Section 10 , Ibid

[33] Sections 11, ibid

The Jordanian Information System Crimes Act No (30) of 2010 is limited in scope. There many acts are not recognized as cyber-crimes such as cyber theft, cyber purchasing, selling and mediation of stolen materials, cyber staking, cyber prepared rubbery, cyber intimidation and extortion, cyber harassment, unjust usage of others belongs, hiding information or counterfeiting certificates of theproperty, cyber defamation, issuing a check without balance, and abuse of trust. However, most of the offences which are provided under the Punishment Code of Jordan, 1960 as traditional crimes can be cyber crimes with rapid technological developments, but they are not covered by the present Law as some amendment to be made here either to the Punishment Code or Cyber Crimes Law. On the same context, it can be observed that the present Cyber Crimes Law, 2010 has no single provision about intellectual property rights or domain names. According to Jordanian jurist Yonis Arab, a Jordanian cyber law specialist, the protection of intellectual property rights and domain names should be the main focus of any cyber law (Arab, 2002: 32), thus the absence of this issue under Jordanian Cyber Crimes Law is questionable?

Section 12 (a) and (b) of the Jordanian Cyber law, 2010 creates another controversial issue among legal jurists in Jordan, where many of them consider it as unconstitutional because it encroach the right of individual to privacy already guaranteed under Article 10 and 18 of the Constitution of Jordan, 1952. This Section grants police forces and judicial police with power of entering cyber suspect's houses for the purpose of search and seizure, which is consider as an investigative procedure conducted only by public prosecutors, except in cases of flagrant delictocrimes that entrance private houses for purpose of search and seizure can be initiated by police forces or judicial police[34] (El-Hiti, 2011).

13. Attack Techniques

Bots generally employ one of several attack methods, but sometimes use multiple techniques to create a network of compromised computers. Some of these approaches are quite sophisticated, such as Phatbot, which can generate a new encryption for itself each time it infects a new system. This makes it difficult for the software to find a common code signature for and thus recognize Phatbot. According to Ken Dunham, director of malicious code for Security Consultancy iDefense, Phatbot has successfully evaded detection by mutating itself from spyware to launch vitriolic DDoS attacks on compromised networks (Lyman, 2004). The following are some of the ways that attackers use to create networks of bots for themselves.

Chat: IRC is the most common used technique, including those in the large Phatbot/Agobot and Sdbot/Robot families as a way to communicate and receive commands from hackers (Leiban, 2002). IRC has a built in mechanism for multicast capabilities which let attackers quickly send commands to all parts of a botnet without writing new code for the bot.

Peer-to-Peer: Many bots take advantage of peer-to-peer communication to infect computers with vulnerabilities. They connect to open-source file sharing technology such as Gnutella and work with the WASTE file-sharing protocol (Brumme, 2004). WASTE uses a distributed directory rather than a central server which lets bots easily find each other and communicate with one another. They can thus exchange hacker commands or other attack-related information among themselves. An attacker can initiate the process by serving as a peer in P2P network sending commands to one bot, which can then pass them onto the others. Thus, hackers don't have to communicate to bots via IRC multicasting. Decentralized-based bot systems are harder for security officials to trace or shutdown than systems using a single IRC source.

Email Attachments/Worms: Many hackers use methods such as email attachments or worms to infect computers. Bots don't replicate or spread on their own, but they can use the worms' functionality to do so. In fact, hackers can spread bots more quickly with worms than with other methods. In addition, Botnets can spread worms faster than worms can spread on their own. The Symantec Security Response team said 2004's Witty worm, which infected and crashed tens of thousands of servers, was probably launched by a botnet. According to Huger, "we saw Witty break out more or less at the same time from a hundred or more machines. The machines were all over the world but they had something in common: they were on our bot list of compromised computers," he noted (Lemos, 2004).

14. Cybercrime Tools

Cyber criminals have developed a wide array of potential tools that have had varyingdegrees of success over the years. The following are a short list of some of these techniques.1) Bots: a bot (short for robot) is a computer on which a worm or virus has installed programs that run automatically and allow cyber criminals access and

[34] See Section 28 of the Jordanian Criminal Procedural Code No (9) 1961, this Section define the flagrant

control. Cyber criminals use viruses or other bots to search for vulnerable computers where they can load their own programs or store data. A botnet is a collection of these infectedmachines that can be centrally controlled and used to launch simultaneous attacks. Spammers, hackers, and other cybercriminals are acquiring or renting botnets, making it harder for authorities to track down the real culprits.2) Key logging: Key loggers are programs that covertly recover the keys typed by a computer user and either stores the data for later access or secretly sends the information to the author. The advantage of a key logger program is that the cybercriminal does not need to trick a user into supplying sensitive information. 3) Bundling: Covertly attaching a virus or spyware to a benign or legitimate download, such as a screensaver or a game. When the computer user downloads and installs the legitimate file, they are unwittingly also giving permission to install the criminal program. 4) Denial of Service: An attack specifically designed to prevent the normal functioning of a computer network or system and to prevent access by authorized users. A distributed denial of service attack uses thousands of computers captured by a worm or Trojan to send a landslide of data in a very short time. Attackers can cause denial of service attacks by destroying or modifying data or by using zombie computers to bombard the system with data until its servers are overloaded and cannot serve normal requests. 5) Packet Sniffers: Software programs that monitors network traffic. Attackers use packet sniffers to capture and analyze data transmitted via a network. Specialized sniffers capture passwords as they cross a network.

6) Rootkit: A set of tools used by an intruder after hacking a computer. The tools allow the cybercriminal to maintain access, prevent detection, build in hidden backdoors, and collect information from both the compromised computer. 7) Spyware: Software that gathers information without the users' knowledge. Spyware is typically bundled covertly with another program. The user does not know that installing one also installs the other. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. 8) Social Engineering: Social engineering is not limited to cybercrime, but it is an important element for cyber fraud. A social engineering trick deceives the recipient into taking an action or revealing information. The reasons given seem legitimate but the intent is criminal. Phishing is an obvious example, a certain percentage of users will respond unthinkingly to a request that appears to be from a legitimate institution. 9) Worms and Trojans: A Trojan is a malicious program unwittingly downloaded and installed by computer users. Some Trojans pretend to be a benign application. Many hide in a computer's memory as a file with a nondescript name. Trojans contain commands that a computer automatically executes without the user's knowledge. Sometimes it can act as a zombie and send spam or participate in a distributed denial of service attack. It may be a key logger or other monitoring program that collects data and sends it covertly to the attacker. Worms are wholly contained viruses that travel through networks, automatically duplicate themselves and send

15. Conclusion & Recommendations

The new law relating cyber crimes in Jordan brings up both substantive and procedural provisions that can be said new for the criminal law environment. The old designed criminal laws in neither Jordan, neither the Punishment Code, 1960 nor Criminal Procedural Code of 1967 are applicable for cyberspace crimes, despite the fact which says that all offences provide in traditional criminal laws can be committed in the cyberspace. However, as abovementioned discussion the present study tries to investigate the way how the Jordanian Cyber Crimes Law, 2010 deals with issues of new types of cyber crimes, where it has been clarified for researchers that the aims that current law enacted for have not been be completed till this moment, thus there is a real need that the future amendments to this law should be made the Parliament and not Governments, simply because the present Interim Cyber Crime Law reflected the prospective of some private centers in Amman and has nothing to do with the social needs, where any law should be the sprit of the society, the law deals with cyber crimes has to be revised by special experts as it contains many techniques and complicated technologies related issues. Hence, upon the outcomes of the present study some recommendation can be summarized as following:

- The modifications for Information Systems Crimes Law No (30) of 2010 are required in some areas that related to specific cyber crimes, such as e-forgery, e-assisting cyber criminalities, and e-fraud; cyber hacking, virus attacks; e-theft, sabotage etc. Otherwise the same modifications can be carried out under the Punishment Code of Jordan, as these offences are provided in this law in their traditional forms.
- The Parliament and the Law Commission in Jordan should revise the provisions of Information Systems Crimes Law No (30) of 2010 by having clear-cut perceptions about the experience of other countries taking into account the fast advances and developments in cyber technologies all over the world. The Jordanian criminal procedures Code also should be amended in order to cover the new procedures and techniques for investigating and prosecuting cyber crimes.

- Cyber law will need to change and evolve as quickly as hackers do if it has any hopes of controlling cyber crime. Law must also find a balance between protecting citizens from crime, and infringing on their rights. The great thing about the internet is how vast and free it is. Will it be able to remain the same way while becoming tougher on criminals? Only time will tell.
- The current cyber law in Jordan has a positive impact on catching criminals in some case when those are employers working within a victimized company, but it is hardly helpful to catch unknown hackers working from anywhere in the world. This is why it is essential to continue studying the experience of other states by applying its legal knowledge and techniques in order to strengthen cyber laws in Jordan and its role in compacting cyber crimes.

References

Abu Jumaa, M. (2012). *Business Ethics and Social Responsibility*. Working Paper Presented in the University of Jadarh, Jordan.

Afifi, A. K. (2013). Computer and Internet Crimes: The Role of the Police in Its Combating. Retrieved from http://www.omanlegal.net/vb/showthread.php?t=290

Ahmad, K. M. (2007). Crimes related to the Gratifying Desire to Use the Computer. In *Regional Conference Booklet "Cyber Crime", June 19-20*.

Al Tamimi, D. A. (2010). *Jordan Introduces New Laws to Tackle the Growth of Cyber- Crime.* Retrieved from http://www.itp.net/582819-jordan-introduces-new-laws-to-tackle-the-growth-of-cyber-crime#.UTvdu6Cea_I

Alaganandam, H., Singh, P. M., & Fleizach, C. (2005). *Cyber criminal Activity.* Retrieved from http://sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf

Almany, N. (2012). *Criminal Investigation, Declining the Rate of Cyber-crime.* Addustour Newspaper, Wednesday, March 28, Issue No. 16059, Forty-sixth Year, Amman, Jordan.

AL-Shawwa, M. (1998). Information Revolution and its Repercussions on Penal Law. Cairo: Dar Al-Nahda Al-Arabiyya.

Arab, Y. (2002). *Computer Crime & Internet: A Summary to the Concept, Scope, Characteristics, Forms and the Procedural Rules of the Prosecution and Evidence*. A Working paper Submitted to the Conference of Arab Security, the Organization of the ArabCenter for Studies and Criminal Research, Held in Abu Dhabi, February 10-12.

Arab, Y. (2002). *Computer Crimes & the Internet*. The Arab Center for Criminal Studies and Research, Abu Dhabi 10-12 / 2.

Barry, M. (2012). *The Age of Interactivity: An historical analysis of public discourses on interactivity in Ireland 1995 – 2009* (Ph.d Thesis). School of Communications, Dublin City University.

Bayoumi, A. F. H. (2004). *Consumer Protection From Commercial Fraud and Counterfeiting in the E-Commerce Contracts through the Internet.* The Third Seminar to Combat Commercial Fraud & Counterfeiting in the Arab Gulf States, Riyadh, September.

Brenner, S. W. (2004). Toward a Criminal Law for Cyberspace: A New Model for Law Enforcement? *Rutgers Computer and Technology Law Journal, 30*(1), 2.

Brumme, S. (2004). *Monitoring the Gnutella Network.* University of Technology, Sydney, Australia.

Burmester, M., Henry P., & Kermes, L. S. (2012). *Tracking cyber-stalkers: A cryptographic approach* (pp. 1, 2 & 4). Retrieved from http://www.cs.fsu.edu/~burmeste/cyberstalking.pdf

Carter, D. L. (1995). *Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin.* Retrieved May 25, 2012, from http://www.fiu.edu/~cohne/Theory

Cavelty, M. D. (2007). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Milton Park, Abingdon, Oxon; New York: Rutledge.

Chadha, S. K. (2010). Impact of Cyber Crime in Society, New Challenges. *International Transaction in Humanities and Social Sciences, 2*(2).

Chen, X. (2010, May 26). Cyber Criminal Activity on the Rise in Turkey. *Data Show, Hürriyet Daily News*. Istanbul.

Council of Europe. (1993). *Recommendation R (91)11 and Report of the European Committee on Crime Problems*.

Deloitte. (2010). Cyber crime: A Clear and Present: Danger Combating the Fastest Growing Cyber Security Threat. Retrieved from http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf

El Sonbaty, E. M. (2007, June 19-20). Cyber Crime - New Matter or Different Category? Legal Harmonization Is The Only Way! In *Regional Conference Booklet "Cyber Crime"*.

El-Hiti, B. M. (2011). *Flagrant Crime & Its Effect on Expanding the Powers of Judicial Police: A Comparative Study between the Jordanian and Iraqi Laws* (Master Dissertation). Middle East University, Amman-Jordan.

El-Shehri, F. bin A. (2011). *Analyzed & Descriptive Study of the Phenomenon of the Internet Crimes*. Retrieved from http://socio.montadarabi.com/t2703-topic

European Commission. (2007). *Toward a General Policy on the Fight against Cyber-crime*. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do:PDF

Fafinski, S., Dutton, W. H., & Margetts, H. (2010). *Mapping and Measuring Cyber-crime* (OII Forum Discussion Paper No 18). The University of Oxford for the Oxford Internet Institute.

Faqir, R. S. A. (2004). *Protection of Accused Rights in Jordan and India: A Comparative Study* (Ph.d Thesis). Law Faculty, Delhi University, Indian.

Fausto, P. (2004). New Challenges for International Rules against Cyber-Crime. *European Journal on Criminal Policy and Research, 10*, 27-37.

Finklea, K. M. (2012, February 15). *The Interplay of Borders, Turf, Cyber-space, and Jurisdiction: Issues Confronting U. S. Law Enforcement.* Prepared for Members and Committees of Congress in U.S. A., Congressional Research Service.

Finnie, T., Petee, T., & Jarvis, J. (2010). *The Future Challenges of Cyber-crime: Volume 5 Proceedings of the Futures Working Group.* Quantico, Virginia.

Geers, K. (2011). *Strategic Cyber Security*. NATO Cooperative Cyber Defense Centre of Excellence, CCD COE Publication, Tallinn, Estonia.

Gercke, M. (2012). *A Report on Understanding Cyber-crime: A Guide for Developing Countries.* Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Goodman, M. D. (1997). Why the Police Don't Care About Computer Crime. *Harvard Journal of Law & Technology, 10*(3).

Goodman, M. D. (1997). Why the Police Don't Care About Computer Crime. *HARV. J. L. & TECH*.

Goodman, M. D., & Brenner , S. W. (2012). *The Emerging Consensus on Criminal Conduct in Cyberspace* (p. 8). Retrieved from http://law.scu.edu/international/File/goodmanbrenner.pdf

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cyber-crime. *Journal in Computer Virology, 2*, 13-20. http://dx.doi.org/10.1007/s11416-006-0015-z

Hawkins, B. L. (2001). Information Access in the Digital Area. *EDUCAUSE Review*, September/ October.

Ionescu, L., Vioric, M., & Blajan, A. (2011). Fraud, Corruption & Cyber Crime in A Global Digital Network. *Economic, Management and Financial Market, 6*(2), 373-380.

Jaishankar, K. (2007). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology, 1*(2).

Kamal, A. (2005). *The Law of Cyber-Space: An Invitation to the Table of Negotiation* (1st ed.). United Nations Institute for Training and Research, Geneva: Switzerland.

Kierkegaard, S. M. (2005). Cracking Down On Cyber-crime Global Response: The Cyber-crime Convention. *Communications of the IIMA, 5*(1).

Kitchin, R. M. (1998). Towards geographies of cyberspace. *Progress in Human Geography, 22*(3). http://dx.doi.org/10.1191/030913298668331585

KPMG International Cooperative ("KPMG International"). (2011). *Cyber Crime: A Growing Challenge to Governments*. Retrieved from http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf

Krone, T. (2005). *High Tech Crime Brief*. Australian Institute of Criminology, Canberra, Australia. Retrieved from http://www.aic.gov.au/documents/6/8/E/%7B68EF707E-CEF8-43FE-B49C-844FBFF2BA0A%7Dhtcb009.pdf

Kumar, V., & Chowbe, S. (2012). *The concept of Cyber Crime: Nature & Scope* (p. 15). Retrieved from http://ssrn.com/abstract=1766238

Leiban, R. (2002). Chat 'Bots' may be hacker tool. *ZDNet Australia*.

Lemos, R. (2004). Alarm Growing over bot software. *CNET News*.

Louis, J. F. (2000). *Statement before the Senate Committee for the Judiciary: Subcommittee on Technology, Terrorism & Government.* Retrieved from http://www.usdoj.gov/criminal/cybercrime/freeh328.htm

Lyman, J. (2004). Worm Variant Parade Marches On. *Tech News World*.

Mamdouh, K. (2009). *Art of Criminal Investigation in Cyber-Crimes.* University House for Thought, Cairo, Egypt.

Maurer, T. (2011). *Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security?* Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School.

McMullan, J., & Rege, A. (2007). Cyber-extortion at online Gambling Sites: Criminal Organization and Legal Challenges. *Gaming Law Review, 11*(6), 648-665. http://dx.doi.org/10.1089/glr.2007.11602

Mitchell, W. (1995). *City of bits: Space, place and the Infobahn.* Cambridge, MA: MIT Press.

O'Hara, G. (2010). Cyber-Espionage: A Growing Threat to the American Economy. *Journal of Communications Law and Policy, 19*.

Olwan, R. (2010). *New Cyber Crime Law in Jordan*. Retrieved from http://www.olwan.org/index.php?option=com_content&view=article&id=402:new-cyber-crime-law-in-jordan-&catid=43:cybercrime&Itemid=68

Panda Security Report. (2010). *The Cyber-Crime Black Market: Uncovered, the Cloud Company.* Retrieved from http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf

Parliamentary Office of Science and Technology. (2006). *Computer Crimes.* Retrieved from http://www.parliament.uk/documents/post/postpn271.pdf

Podgor, E. S. (2002). International Computer Fraud: A Paradigm for Limiting National Jurisdiction. *UC Davis Law Review, 35*. Retrieved from http://ssrn.com/abstract=295173

Rosenzweig, P. (2009). *National Security Threats in Cyberspace*. A Workshop Jointly Conducted by: American Bar Association Standing Committee on Law and National Security and National Strategy Forum, June 4-5. Retrieved from http://nationalstrategy.com/portals/0/documents/nationalsecurity.pdf

Samarah, M. (2008). Cyber Crime. *Journal of Information Security*, (29).

Schell, B. H., Dodge, J. L., & Moutsatsos, S. (2002). *The hacking of America: Who's doing it, why, and how?* New York: Quorum.

Schjolberg, S., & Ghernaouti-Helie, S. (2011). A Global Treaty on Cyber-security and Cyber-crime (2nd ed.). AiTOslo.

Shakir, Y. (2011). *Mens Rea (Intentional) Element under Jordanian Act on Crimes of Information Systems.*

Smith, R. G., Grabosky, P., &Urbas, G. (2011). *Cyber Criminal on Trial*. Cambridge University Press.

Su, C., & Holt, T. J. (2010). Cyber bullying in Chinese Web Forums: An examination of nature and extent. *International Journal of Cyber Criminology, 4*(1&2).

The Statement of the Jordanian Minister of Communications and Information Technology. (2012). Retrieved from http://www.sarayanews.com/object-article/view/id/111219/title

The UN Manual on the Prevention and Control of Computer-Related Crime. (1994). Retrieved from http://www.uncjin.org/Documents/EighthCongress.html

Wakefield, M. A., & Rice, C. J. (2008). *The impact of cyber-communication on today's youth (ACAPCD-14).* Alexandria, VA: American Counseling Association.

Wall, D. S. (2007). *Cyber-crime: The Transformation of Technology in the Networked Age.* Cambridge: Polity Press.

Watch, M. B. (2001). *The Fight against Cyber-crime.* Retrieved from http://www.pcw.co.uk

Yar, M. (2005). The Novelty of 'Cyber-crime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4). http://dx.doi.org/10.1177/147737080556056

Yucedal, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity & Lifestyle Exposure Theories* (Ph.d Thesis). Kent University.