International Journal of Cyber Criminology
Vol 7 Issue 1 January - June 2013

Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010

Raed S. A. Faqir[1]
Balqa Applied University, Jordan

Abstract

Cyber crime poses a critical task for police force and judicial police in Jordan because the unique technical nature of this crime. The threat of cyber crimes can not be reduced unless all the members of Jordanian criminal justice system are aware about the developed and advance technology of computer and electronic devices. One decade ago, there has been an actual focus within the Jordanian criminal justice system on computer- enabled offences. This so-called "hi-crime", including internet crimes, cyber-crimes, crimes committed by electronic devices and computer-related crimes, has occupied a high attention of the Jordanian Legislators because computers have become the boon of vital activities of everyday human life and the Information Systems Crimes Law No (30) of 2010 (ISC Act, 2010) was promulgated. This paper aims to determine the effectiveness of legal mechanism in Jordan for combating cyber-crimes and computer-related crimes, law relating cyber crimes with special focus on ISC Act, 2010 and will identify the impact of cyber crimes on criminal law, and limitations of Jordanian ISC Act, 2010.

Keywords: Cyber crimes, Cyber Laws, Legal and Legislative Challenges in Jordan.

Introduction

Cyber-crimes represent a real challenge to all criminal justice systems all over the world including Jordan. In Jordan, there is a real rise in the number of cyber-crimes; the record of the Jordanian Statistics of Public Security shows more than 1103 cyber-crimes were committed in the Kingdom until the end of November 2011 (Statement of the Jordanian Minister of Communications and Information Technology, 2012). According to statistics of the Criminal Investigation Department in the Jordanian Public Security the number of cyber crimes since the beginning of the year 2012 reached 47 cases, 17 cases of impersonation and e-defamation, and 12 cases e-threatens, two cases of the electronic financial frauds, and 16 e-mail theft cases. In 2011, the cyber-crimes are classified as 427 cases of impersonation and e-defamations, 350 cases of threats and defamation, and 21 issues of e-financial fraud, 40 cases of e-mail thefts, 3 cases of electronic data and internet servers of thefts, and two cases of child abuse on the internet (Almany, 2012).

One decade ago, there has been an actual focus within the Jordanian criminal justice system on computer- enabled offences. The first law in Jordan to investigate and prosecute

[1]Assistant Professor of Law at Zarqa University College, School of Law, Balqa Applied University, Jordan. Email: fageerjo@yahoo.com

cyber-crimes and computer- related crimes is Electronic Transactions Act No (85), 2001, which use to deal with these type crimes by indirect way, and the focus of law is about the electronic transactions from commercial and civil prospective rather than criminal. In 2010, the Information Systems Crimes No (30) law (thereafter ISC Act, 2010) was done as an amendment to the Electronic Transactions Act No (85), 2001. Even though this law is a pioneering law to the field of cyber crimes it does not provide adequate relief. The ISC Act No (30) of 2010, despite the shortages and defects that it has, still represents a dramatic shift in the legal system of Jordan.

This paper deals with cyber crimes and its challenges in the criminal justice system of Jordan, the legislation in Jordan dealing with crimes in cyberspace and computer-enabled offences, as well as other crimes committed by the use of electronic devices. The Information Systems Crimes Act No (30) of 2010 has been dealt in detail with an analysis of its strengths and weakness. The analysis of the effectiveness of the Jordanian Information System Crimes Act, 2010 and the legal mechanism for compacting cyber offences in Jordan is based on data that are gathered through published annual Reports, Articles published in books, journals and newspapers etc. In addition, electronic articles, books and materials posted on Internet websites are consulted.

The importance of present paper emanates from the reality of that the applied laws on cyber issues within the legal system of Jordan can not be deemed as a foundation for investigating and prosecuting cyber-crimes. In Jordan, judges, prosecutors, lawyers and law enforcements are in dilemma because the insufficient and vague cyber-legislations, the traditional legal provisions contained in Punishment Code, 1960 and Criminal Procedural Code, 1961 are incompatible to deal with cyber crimes and they need to be revised and amended. Additionally, the ISC Act, 2010 suffers lot from legal and linguistic defects, less coverage of cyber-crimes, formula problems, and absence of the procedural rules, therefore its provisions have to revised and updated by the parliament, as well as there is a need produce it as a permanent law.

Information System Crimes Law No (30) of 2010: Salient Features

The ISC Act, 2010 has been adopted by the government of Jordan as interim law in order to fill up the lacunae in the Electronic Transactions Act No (85), 2001. The ET Act, 2001 suffered from lot of defects, especially in the filed of criminalization and punishment of criminal cyber activities. The focus of this law was on e-commerce and no provisions were designed for computer related offences, and the enactment of ISC Act, 2010 was as necessary as it attuned to the Jordanian needs (Nafi & Amawi, 2002). The ISC Act, 2010 has been formulated in a substantive way where cyber offences were defined and enumerated along with penalties, but without a procedural support.

The ISC Act, 2010 is 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 Act of 2010 is very simple, it totally has 18 sections without chapters, and it embodies two types of substantive and procedural rules. This Act begins with preliminary definitions; describe cyber crimes under sections 3 to 12 and lays down penalties therefore. The Act also is applicable within the entire territories of Jordan and except otherwise provided, the capability of ISC Act, 2010 is made even in the case of crimes committed outside Jordan.

Table 1. Cyber related Crimes as provided by the Jordanian Interim Information Systems Crimes Law No (30) of 2010

No	Offence	Section of ISC Law
1.	Unauthorized Access to Information System	Sec.3 (a)
2.	Tampering Information Systems through Destroying, Deleting or Copying	Sec.3 (b)
3.	The Act of Impersonation	Sec.3 (b)
4.	Impeding the Information System by Jamming or Disruption	Sec.4
5.	Interception of Information by Unauthorized Electronic Eavesdropping	Sec.5
6.	Unlicensed Obtaining Credit Card and Banking Information	Sec.6 (a)
7.	Unlicensed Using Credit Card and Banking Information	Section 6 (b)
8.	Unlicensed Using Credit Card and Banking Information by Insiders	Section 7
9.	Pornography and Sexual Exploitation of Children	Section 8(a)
10.	Activities of Online Prostitution	Section 8(b)
11.	Using Information Systems for Seducing Psychopaths or Mental Handicaps for Online Prostitution or Pornography	Section 8(c)
12.	Promotion of Online Prostitution	Section 9
13.	Facilitation or Support of Terrorist Acts	Section 10
14	Promotion of Terrorist Ideologies	Section 10
15	Illegally Access to National Security, Safety and National Economy Information	Section 11 (a)
16	Illegally Access to National Security, Safety and National Economy Information for the Purpose of Abolishing, Destroying, Alerting or Copying.	Section 11 (b)

As shown in Table 1 some remarkable features of the ISC Act, 2010 are revealed: criminalization of new cyber-crimes that were unknown under the legal system of Jordan, definition of cyber crime, protection data privacy, criminalization new types of child pornography, cyber banking and financial crimes, cyber terrorism and authorizing police forces and juridical police for investigation of cyber crimes, by empowering them with act of searching and seizing those crimes. However, the coverage of cyber crimes under this Act is not complete in comparing with the legislation of other countries. Thus any future amendment to this law should take the foreign legislations and experiences in to account.

Table 2. Penalties and Punishments for Cyber related Crimes as provided by the Jordanian Interim Information Systems Crimes Law No (30) of 2010

No	Offence	Fine	Imprisonment
1.	Unauthorized Access to Information System	100 -200 JD	7 days to 3 months
2.	Tampering Information Systems through Destroying, Deleting or Copying	200-1000 JD	3 months to one Year
3.	The Act of Impersonation	200-1000 JD	3 months to one Year
4.	Impeding the Information System by Jamming or Disruption	200-1000 JD	3 months to one Year
5.	Interception of Information by Unauthorized Electronic Eavesdropping	200-1000 JD	One month to one Year
6.	Unlicensed Obtaining Credit Card and Banking Information	500-2000 JD	3 months to 2 Years
7.	Unlicensed Using Credit Card and Banking Information	1000-5000 JD	One at Least
8.	Unlicensed Using Credit Card and Banking Information by Insiders	2000-10000 JD	Two years at Least
9.	Pornography and Sexual Exploitation of Children	300-5000 JD	Three Months at Least
10.	Activities of Online Prostitution	1000-5000 JD	Two Years at Least
11.	Using Information Systems for Seducing Psychopaths or Mental Handicaps for Online Prostitution or Pornography	5000-15000 JD	Temporary Hard Work Imprisonment
12.	Promotion of Online Prostitution	300-5000 JD	Not less than 6 Months
13.	Facilitation or Support of Terrorist Acts	No fine	Temporary Hard Work Imprisonment
14.	Promotion of Terrorist Ideologies	No fine	Temporary Hard Work Imprisonment
15.	Illegally Access to National Security, Safety and National Economy Information	500-5000 JD	Not less than 4 Months
16	Illegally Access to National Security, Safety and National Economy Information for the Purpose of Abolishing, Destroying, Alerting or Copying.	1000-5000 JD	Temporary Hard Work Imprisonment

As seen from the Table 2, it can be observed that the Jordanian Interim Information Systems Crimes Act No (30) of 2010 focuses on the major cyber-crimes, but still has not covered entirely all known computer related crimes. Section 3 of the ISC Act may be considered as an important section; it criminalizes all acts of un-authorized access or violation of an authorization to a website or information system, and panelizes those actions with the imprisonment of not exceeding three months, or by a fine of not exceeding two hundred JD (Jordanian Dinar).[2] In paragraph (b) of Section (3) the

[2] Section 3 (a) of the Jordanian Information Systems Crimes Act No (30) of 2010 provides that: A- Anyone who intentionally accesses a website or information system in any manner without authorization or in violation or excess of an authorization, shall be punished by imprisonment for a term not less than one

legislator made the penalty much severe than stipulated in paragraph (a) of the same Section, the provided penalty for un-authorized access to a website or information system for the purpose of canceling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information or stopping or disabling the operation of an information system, changing a website or canceling, destroying or altering its content or assuming its identity or the identity of its owner is imprisonment for not exceeding one year or a fine of not exceeding one thousand JD.[3]

Moreover, it is inferred from the Table 2 that: Section 4 of the ISC Act prohibits the actions of installment, publication or usage of any sort of programmes through information systems related with data or information, or obstruct, interfere, hinder, stop the operation of an information system or prevent access to it, while the punishments for committing such type of cyber-crimes are lenient[4]. Section 5 of the Information Systems Crimes Act deals with acts of capturing, intercepting or eavesdropping on sent information through an information network or any information as cyber-crimes, but it does penalize such crimes with sever punishments as made under section 4.[5] Un-authorized obtaining or using of data or information are classified under the Act as cyber-crimes, especially when these acts related to credit cards or data or information that is used in execution of electronic financial or banking transactions, while they are punished somehow with sever punishments.[6]

---

week and not exceeding three months, or by a fine of not less than (100) one hundred Dinars and not exceeding (200) two hundred Dinars, or both punishments.

[3] Section 3 (b) of the Jordanian Information Systems Crimes Act No (30) of 2010 provides that: Where the access stipulated in paragraph (a) of this Article is for the purpose of canceling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information or stopping or disabling the operation of an information system, changing a website or canceling, destroying or altering its content or assuming its identity or the identity of its owner, the perpetrator shall be punished by imprisonment for a term not less than three months and not exceeding one year or by a fine of not less than (200) two hundred Dinars and not exceeding(1000) one thousand Dinars, or both punishments.

[4] Section 4 of the Jordanian Information Systems Crimes Act No (30) of 2010 provides that: Anyone who installs ,publishes or uses intentionally a program through an information network or information system, with the purpose of canceling, 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 canceling it, destroying it, or altering its content or operating it, assuming its identity or the identity of the owner without authorization or in violation or excess of the authorization shall be punished by imprisonment for a term not less than three months and not exceeding one year or by a fine of not less than (200) two hundred Dinars and not exceeding(1000) one thousand Dinars, or both punishments.

[5] Section 5 of the Jordanian Electronic Transactions Law No. 85 of 2001 provides that: Anyone who intentionally captures, interferes or intercepts what is transmitted through an information network or any information system shall be punished by imprisonment for a term not less than one month and not exceeding one year or by a fine of not less than (200) two hundred Dinars and not exceeding (1000) one thousand Dinars, or both punishments.

[6] Section 6 (a) and (b) of the Jordanian Information Systems Crimes Act No (30) of 2010 provides that: A- Anyone who intentionally and without authorization obtains through an information network or any information system data or information relating to credit cards or data or information that is used in execution of electronic financial or banking transactions shall be punished by imprisonment for a term not less than three months and not exceeding two years or by a fine of not less than (500) five hundred Dinars and not exceeding (2000) two thousand Dinars, or both punishments. B- Anyone who intentionally uses through an information network or any information system data or information relating to credit cards or data or information that is used in execution of electronic financial or banking transactions to obtain to

The Effectiveness of the Information Systems Crimes Act, 2010 (ISC Act)

1. Points of Strength

The Jordanian ISC Act, 2010 is the first special legislation with the jurisdiction of Jordan that deals with issues of cyber crimes and activities, despite of the criticism made against it but still it has guarantees the minimum framework for cyber offences. There are various positive aspects of the Act which is explained below:

Firstly, the essence of these provisions for e-transactions of different forms and types are recognized as protected and safeguarded targets, thus e-commerce and e-business as well as e-mailings became legally recognized and reliable form of transactions that would be admissible in courts of Jordan.

Second, public and private organizations, juridical and private individuals and persons are empowered with practicing all types of electronic transactions safely upon the protection provided by the ISC Act, 2010.

Third, the provisions of ISC Act define the elements of information systems crimes, especially because these types of crime have different elements in comparing with traditional offences which are not specified by the traditional Punishment Code, 1960.

Fourth, the Act redresses the legislative loopholes for combating the international crimes committed through the use of information systems or informatics networks, such as promotion of prostitution or invasions against banking systems or accounts.

Fifth, the Act guarantees the electronic freedom by surrounding it with social security of the protection of the internet users against cyber activities, by punishing persons involved with commission those crimes (Al.Syeed, 2013).

Sixth, pornography and sexual exploitation of children, Activities of Online Prostitution and promotion of terrorist ideologies have been recognized as cyber crimes and were given sanction in the Act (Abu Sharkh, 2013).

Seventh, the ISC Act, 2010 also addresses vital issues of illegal access to national security; safety and national economic information for purpose of abolishing; destroying, alerting or copying and proper sanctions were designed for in the Act. The Act focuses also on other important issues of banking and financial security related to unlicensed obtaining and of credit card and banking information, where specific sanctions were imposed for under the Act. [7]

Eighth, under the ISC Act, 2010, it shall now be possible to impose harsh punishments of imprisonment ranges from seven days to temporary hard work and fine ranges from 100 to 5000 thousand JD for various information system crimes. The Act gives juridical individuals and persons the choice to go for remedy for breaking their information security or monetary damages. [8]

Ninth, the ISC Act, 2010 also ensures the protection of commercial transactions and the stability of the financial transactions and encourages the use of electronic information systems. The Act also provides the minimum limits of protection to the information network and its users, furthermore it takes into account the non-criminalization of every activity related to freedom of expression or personal freedoms unless those acts are already

oneself or others the data, information, assets or services of others shall be punished by imprisonment for a term not less than one year or by a fine of not less than (1000) one thousand Dinars and not exceeding (5000) five thousand Dinars, or both punishments.

[7] See Sections 6 (a) and 7 of the Jordanian Information System Crime, 2010

[8] See Sections 3, 4, 5, 6, 7, 8, 9, 10 and 11 of the Jordanian Information System Crime, 2010

criminalized under other legislations in force, especially if they are committed intentionally by using electronic means.[9]

Tenth, the Act has not imposed punishments on telecom networks operators, service providers, maintenance service providers and owners of websites who have not intentionally committed, aided and abetted in the commission of a cyber crime in order to ensure the continuation of promoting the use and development of electronic means.[10]

2. Points of Weakness

The ISC Act, 2010 though the above mentioned points of strength, it takes negative stand towards many cyber issues. It has inaccurate solutions for many practical issues and loses the coverage for many internationally recognized cyber offences as well as potential activities of futuristic nature of the cyberspace's offences. The points of weakness within the provisions of this Act are:

First, the Act has left many significant issues related to cyber stalking or online harassment, cyber threat, spamming, dissemination of obscene materials, the stealing of inside information for fraudulent exploitation such as scamming, and moreover intellectual property rights, copyrighting and trade marking or patenting of electronic information, among other things that have not addressed by the Act.

Second, the provisions of ISC Act, 2010 misses very important issues of cyberspace and electronic transactions those are related to protection of trade marks and domain names against online illegal forgery, counterfeiting and copying, which are not criminalized or sanctioned at all under this Act.

Third, the ISC Act, 2010 is limited in its scope, there are no provisions for criminalizing and punishing for acts related to computer-related fraud, forgery and identity-related crimes, the Act is further ineffective as it loses dealing cyber extortion and extortionate threats.

Fourth, the ISC Act, 2010 has not established a proper legal mechanism to combat all possible criminal activities carried out by the use of information systems and information networks, thus with the absence of an organized mechanism to respond to cyber threats serious cyber attacks may take place at any moment against the vital websites of our agencies or ministries, or organization in both public and private sectors.

Fifth, the Act ignores the criminalization of gambling while criminalized online prostitution and temptation. It loses to clarify the penalty of constructing terrorist websites or commission organized crimes by using information systems and information network. These controversial lacunas have many forms of unclear terms, penalties, and fines.

Sixth, the Act gives extra authority to judicial police, the provisions of this law contains ambiguous authorities that vested to police officers and judicial police men and some how are out of the scope of section 8 (1) of the Criminal Procedure Code, 1961, by which the main duty of judicial police is crime inquiry and evidence collection (Thunaibat, 2011).

Seventh, the ISC Act, 2010 contains several restrictive aspects that can be used to harass electronic media. The Act in its current form may lead to weakening the reputation of Jordan as a free and open society, especially as it contains number of sections formulated vaguely which may hinder freedom of expression over the Internet and restrict the ability of journalists to cover the news. In general, the Act vests the public authorities with broad

[9] See Sections 4, 5 and 6 of the Jordanian Information System Crime, 2010
[10] See Section 81 of the Jordanian Punishment Code, 1960

powers to restrict the flow of information and public debate (Committee for Protection of Journalists, 2010).

Eighth, Section 12 and 13 of the ISC Act, 2010 are criticized, because the restrictions imposed by them on the freedom of journalism. Section 12 of this Act imposes a penalty on any one who may be known any sort of "data or information that is not available to the public and affecting national security or foreign relations of the Kingdom, public safety or the national economy" through the use of the Web site or the information system. Section 13 allows for law enforcement officers to inspect offices that manage sites on the Internet and inspect devices without prior approval of the public prosecutor (Committee for Protection of Journalists, 2010).

Ninth, some of the provisions of ISC Act, 2010 are vague, especially those relating to the protection of privacy, such provisions misses the clarity, specificity and accuracy of drafting, where they are omitting other forms of cyber offences concerning the protection of the right to privacy, by which becomes suffering from legislative deficiency (Al-Momani, 2010).

Tenth, the Human Rights Watch criticized the ISC Act, 2010 because it imposes more restrictions on public freedoms and freedom of expression in Jordan and it alleges that the Act is inequitable and against the international conventions guarantee the right of all individuals to freedom of expression, such as the International Covenant on Civil and Political Rights, which the Jordan is a party to (CNN, 2010).

Eleventh, the ISC Act, 2010 needs to be amended in order to provide a suitable criminal protection against offenses arising from the use of computers and the information revolution in more comprehensive way. Any amendment to this Act shall take into account the current obstacles of the application of justice with regard to the means of electronic proofs, thus as the procedural application of ISC Act relies on the Cr. P Code, 1961, there is a need to amend Cr. P Code to make more accommodated to the electronic inquisitorial and seizure procedures as well as inspection means. Moreover, the problems of implementation of ISC Act are not only related to the defections of Cr. P Code, 1961 but also the Jordanian Evidence Code, which has to be amended in order to deal electronic proofs for cyber crimes in the same way in case of traditional crimes.

The ISC Act, 2010 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. The absence of procedural aspects of the ISC Act, 2010 expose the application of this Act to jeopardy and makes as ineffective in dealing with the recent advances in the field of technology and telecommunication. The authority of public prosecutors to investigate cyber activities and to interrogate, arrest, search and seizure, etc have not been provided for in this law and all procedural issues were referred to the Cr. P Code, 1961. The new Act is characterized with its shortage of coverage, because lot of internationally recognized cyber crimes were not covered and some of them were not properly provided, moreover some of other crimes were dealt with in traditional way as contained in the Jordanian Punishment Code, 1960.

The Act, upon the comprehensive and an overall analysis, reveals a shortage of coverage and deepness of several matters relating to cyber law. Despite the Jordanian Law is given the name of "Information Systems Crimes Act" still many legal matters like privacy concerns, freedom of expression, freedom of media, trade marks and domain names conflicts, crime of defamation, right of person to access information, online rights, investigative powers of judicial policemen, online money laundry, legal mechanism for

combating future and potential type of cyber crimes, computer-related fraud, forgery and identity-related crimes, cyber stalking or online harassment, cyber threat and spamming etc have not been addressed by the ISC Act, 2010. Finally, the Act still suffering from the absence of the proper legal mechanism for its implementation, especially with lack of the procedural aspects of the law and referring the issue to rules contained in Criminal Procedural Code, 1961 which they are more suitable for traditional offenses than those provided in the ISC Act.

Conclusion and Recommendations

The problems of ISC Act, 2010 seem to be multi faceted in nature. Firstly, the Jordanian ISC Act is highly deficient from different angles. Thus, there is an absence of proper legal foundation for investigation and prosecution of cyber offenses and digital evidences in court of Jordan are not treated as equivalent to traditional and physical evidences. Secondly, there is a need to amend the ISC Act, 2010, the Punishment Code, 1961 and Criminal Procedural Code, 1961 in order to enable justice agents in dealing with cyber offenses, moreover to subject lawyers, judges, prosecutors and police officers to special training. Thirdly, the cyber studies, cyber specialty and cyber legal system capabilities are very weak in Jordan, therefore legislations and experiences of other nations for investigating and prosecuting cyber crimes have to be consulted for the purpose of enactment of sufficient and effective legal framework to the cyberspace's crimes in Jordan. Fourthly, the cyber crimes compacting strategies in Jordan are deficient and need an actual overhaul. Fifthly, most of cyber offences against persons are not dealt accurately and the have maltreated under the Jordanian ISC Act, 2010, those are harassment via e- mails, email spoofing, cyber-stalking, dissemination of obscene material, online Defamation, indecent exposure, cheating and fraud, breach of confidentiality and cyber-espionage, therefore such offences must be given more attention in any future amendments to this Act.

The ISC Act, 2010 should be amended in some manner that covers all possible crimes of cyber space, such as computer related crimes, including computer forgery, assisting cyber criminals, and computer fraud; crimes of access, embodying cyber hacking, and virus attacks; information and data offences, including cyber-theft, sabotage, modification, and interception; network related crimes, including sabotage and interference.

The provisions of Jordanian ISC Act, 2010 have to be revised by Parliament in order to make major amendments necessary for reducing the legislative vacuums and defects in the present Act. Any amendments to this Act should cover both the substantive and procedural rules, and in particular to provide expressly a change in section 12 (a) and (b) which expands the powers of police forces and judicial police searching and seizing cyber-crimes, this power should be always in the hand of public prosecutor for more guarantees to the constitutional rights of individuals.

Provisions of ISC Act, 2010 have nothing new more than what has been provided in traditional criminal laws, thus the governmental enacted ISC Act should entirely revised and amended by the new 17th Parliament of Jordan in order to make it more effective as a remedy for all possible internal or external cyber activities. Before doing so all related sectors in the country should be consulted not only inside the criminal justice system, but also the private sector. The ISC Act, 2010, shall be modified in order to contain more specific procedural rules that are necessary for its implementation.

Specific cyber offenses of harassment via emails, email spoofing, cyber stalking, dissemination of obscene material, online defamation, indecent exposure, cheating and fraud, breach of confidentiality, cyber-espionage, offences against domains names, phishing and pharming should be given more attention in any future amendments to this Act. The traditional 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. Any amendments to the ISC Act should take into account the role of the police in controlling the production of computers, to vast all persons who work in the field of informatics the power of judicial police and require net providers the prior permission of police, as well as to strengthen the role of the police in the framework of international cooperation to fight cyber crimes

Members of both the Bar and the Bench in Jordan shall be more specialized in dealing with cyber crimes by subjecting them to regular and special cyber training courses. Therefore a center for cyber space laws is suggested to be established in Amman for this purpose. In conclusion; as it has been seen through this that the aims behind the enactment of Jordanian ISC Act, 2010 have not been achieved, such aims to be completed only by the amendments of Parliament not Governments, simply because the Interim present Act was a simple production of private center in Amman, it is hoped that within short time the Act be reviewed by special experts in this field.

References

Abu Sharkh, A. K. (2013). Freedom of Expression on the Internet. Retrieved on 28 April, 2013 from http://abusharkh-jo.com/?page_id=423

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

Al-Momani, N. (2010). Jordanian Information Systems Crimes Act and the Right to Privacy. Awareness & Empowerment Unit, the National Centre for Human Rights, Amman, Jordan. Retrieved on 28 April, 2013 from http://www.nchr.org.jo/arabic

Al. Syeed, R. M. (2013). Cyber Crimes and Law. *Addustour Newspaper*, No. 16452 Forty-Seventh Year, Issued on Tuesday 20 Jumada II 1434 H, April 30, 2013.

Committee for Protection of Journalists, Information System Crimes Act: It weakens Jordan's Image Abroad (2010). Retrieved on 26 April, 2013 from http://www.gerasanews.com/index.php?page=article&id=32573

CNN Arabic. (2010). Are the Laws of "Information" in Jordan Seeking to Crack Down Freedoms? Retrieved on 26 April, 2013 from http://arabic.cnn.com/middle_east

Nafi, B., & Amawi, I (2002). E-commerce As Seen by the Jordanian Legislator. Retrieved on 26 April, 2013 from www.lawjo.net/vb/attachment.php?attachmentid=128&d

Statement of the Jordanian Minister of Communications and Information Technology (2012). Retrieved on May 25, 2012 from http://www.sarayanews.com/object-article/view/id/111219/title

Thunaibat, G. (2013). Information System Crimes Law, 2011. Retrieved on 28 April, 2013 from http://www.dr-ghazi.com/