BRILL
NIJHOFF

GLOBAL JOURNAL OF COMPARATIVE LAW 5 (2016) 226-261

GJCL
brill.com/gjcl

Enacting Cybercrime Legislation in an Endeavour to Counter Cybercrime in Palestine

Mustafa Abdelbaqi (*Ph.D*)
Palestinian Bar Association; Birzeit University, Palestine; Max Planck Institute for Foreign and International Criminal Law, Germany
mustafa_abdelbaqi@yahoo.com

Abstract

The rapid development of information and communication technology has increased the opportunities for criminals to commit cybercrime. As many countries, Palestine faces problems countering cybercrime from both the legislative and technical perspectives. Palestinian courts deal with the matter using one of two approaches. In some instances, public prosecutors choose not to prosecute the act due to the fact that there is no provision of law applicable to the conduct. In others, they adapt the related conventional provisions of the Criminal Code to the conduct. To counter cybercrime, the Palestinian legislature should enact a cybercrime law, which is compatible with the Council of Europe Convention on Cybercrime, or incorporate the Arab Convention on Combating Information Technology Offences of 2010 in the Palestinian legal system. Legal reform is crucial, but not sufficient. Technical approaches, public awareness and ethical online education are vital as well. Meanwhile, the cooperation of the international community, as a whole, including the different formal and informal agencies in each country becomes necessary.

Keywords

Cybercrime – Council of Europe Convention on Cybercrime – Arab Convention on Combating Information Technology Offences – Palestinian Draft Computer Transaction Law – computer offenses – copyright offences

* My thanks to the Palestinian Zamalah Program for financing the Visiting Scholarship to Belgium (July-August, 2015); to Prof. Dr. Kim Vanderborght for hosting me in the premises of the Free University of Brussels (VUB) for two months; to Prof. Dr. Catherine Grosso and Dr. Cailin Mackenzie for reading and commenting on an earlier version of this paper.

 | DOI 10.1163/2211906X-00502003

1 Introduction

Computer and internet technology have affected daily life in developed countries over the last two decades,[1] and more recently, in developing countries as well. More than 2.7 billion people (about 40% of the world's population) used the internet regularly in 2013.[2] As a result, the world is now a small village, "[I]n the network world, no island is an island."[3] Online banking; e-commerce; e-voting; communications with family and friends; and the administration of transportation, electricity, water supply and other critical infrastructure systems[4] are just a few examples of the widespread use of information and communication technologies (ICTs). This rapid development of ICTs has increased the opportunities for criminals to commit new and old types of crime. In particular, the interaction between computers and communication systems has resulted in the birth of cybercrime.[5]

There is no universally accepted single unified definition of cybercrime.[6] This lack of a unified definition of cybercrime interferes with the efforts of the international community to combat it.[7] In fact, the United Nations noted

1 The widespread use of computers and internet began in the developed countries in the mid-nineties. Before that the use of the internet was limited to the elite, e.g. academics and the rich people.

2 Buono, Laviero, Fighting cybercrime through prevention outreach and awareness, ERA, 2014. http://download.springer.com/static/pdf/ (cited August 15, 2015).

3 Goodman, Marc, International Dimensions of Cybercrime (Chapter 17), (311– 339) in: Ghosh, S, and E. Turrini (eds.), Cybercrimes: A Multidisciplinary Analysis, Springer- Verlag Berlin Heidelberg 2010.

4 Maitra, Amit K., Offensive cyber-weapons: technical, legal, and strategic aspects. http://link.springer.com/article/10.1007/s10669-014-9520-7 (cited August 16, 2015).

5 The terms computer crime, electronic crime, digital crime, info highway crime, high-tech crime, internet crime and cybercrime are mainly used interchangeably. They describe the illegal activities taking place in cyberspace or ones associated with computer networks. For further info on this subject, see Maghaireh, Alaedine Mansour Sofauq, Jordanian Cybercrime Investigations: a Comparative Analysis of Search for and Seizure of Digital Evidence, unpublished Ph.D Thesis, Faculty of Law, University of Wollongong, 2009. http://ro.uow.edu.au/thesis/3402. p. 2. (last visited July 14th, 2015).

6 Gordon, Sarah and Richard Ford, On the Definition and Classification of Cybercrime, Springer-Verlag France (2006). http://vxheaven.org/lib/pdf/On%20the%20definition%20and%20classification%20of%20cybercrime.pdf (cited July 20, 2015).

7 Some scholars think that the vagueness of definitions on cybercrime could be referred back to the high rate of technological progress. See Makela, Liisa, Information Society and Penal Law, Section I – FINLAND, Preparatory Colloquium Verona (Italy), 28–30 November 2012. http://www.penal.org/sites/default/files/files/RV%20-%204%20new.pdf (cited July 20, 2015).

that the lack of global agreement on the legal definition of criminal conduct would make it difficult to report consistently on its nature and extent from one country to another and to monitor trends in an informed manner.[8] The Oxford Dictionary of Law defined cybercrime as: "crime committed over the internet." Researchers defined it as a "criminal activity conducted in cyberspace by means of Internet technology."[9] A scholar defined it as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecution."[10] Another one defined it as "any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network.[11] A third one defined it as "any illegal activities simultaneously associated with information technologies and cyberspaces, intentionally perpetrated for tangible and/or intangible benefits and primarily motivated by self-interest."[12] According to the last definition, not every crime committed with the involvement of a computer is a cybercrime. For example hitting somebody using the keyboard is not a cybercrime.[13] Every year cybercrime causes tens of billions dollars in financial damage. This exceeds the total amount of damages resulting from physical crime.[14] The Federal Bureau of Investigation (FBI) considers high-tech crimes to be the most significant crimes confronting the United States.[15] The true extent of cybercrime is difficult to assess mainly because the victims are reluctant to report cybercrimes, especially in the economic and financial

8 Alkaabi, Ali, Dealing with the Problem of Cybercrime (pp. 1–18), in: Ibrahim Baggili (Ed.), Digital Forensics and Cybercrime, Springer, Abu Dhabi, UAE, 2010.

9 Curtis, Glenn (*et. al*), Cybercrime: an Annotated Bibliography of Select Foreign-Language Academic Literature, Federal Research Division, Library of Congress, November 2009.

10 Carter, J. and Audrey Perry, 'Computer Crime' (2004) 41 American Criminal Law Review PP. (313– 314).

11 Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000), United Nations. http: //www.uncjin.org/Documents/congr10/10e.pdf page 4 (cited August 20th, 2005).

12 Maghaireh, supra note 5, at 6.

13 Maghaireh *Ibid,* P. 7.

14 Gercke, Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU Telecommunication Development Bureau. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (cited July 17, 2015).

15 Comey, James B., Remarks before the RSA Cyber Security Conference, Federal Bureau of Investigation, San Francisco, CA, February 26, 2014. https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-closing-the-gap-in-cyber-security. (cited September 10, 2015).

fields. Businesses fear that negative publicity could damage their reputation.[16] The other significant reason for the difficulty in assessing the extent of cybercrime is that some cyber offences are not yet universally criminalized.[17]

2 Statement of the Problem

Palestine faces problems countering cybercrime from both the legislative and technical perspectives. The International Telecommunication Union (ITU)[18] created the Cyberwellness Profile of the State of Palestine in December 2012.[19] The ITU found that no specific legislation on cybercrime has been enacted. It also found that Palestine is not well equipped in the domain of cybersecurity and infrastructure. Among other issues, Palestine does not have any officially recognised national Computer Incident Response Team (CIRT); it does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognised cybersecurity standards and there is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals. The ITU found that Palestine has no national governance roadmap for cybersecurity. Concerning national benchmarking, Palestine does not have any officially recognised national benchmarking to measure cybersecurity development. There is no officially recognised national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines. Palestine does not have the required number of public sector professionals certified under internationally recognised certification programs in cybersecurity. Palestine does not have any government and public sector agencies certified under internationally recognised standards in cybersecurity. Concerning cooperation, there is no framework to facilitate sharing of cybersecurity assets across borders or with other nation states. Palestine does not

16 Drewer, Daniel and Jan Ellermann, Europol's data protection framework as an asset in the fight against cybercrime, ERA. http://link.springer.com/article/10.1007/s12027-012-0268-6. (cited August 15, 2015).

17 CoE Technical Report 2004 (Summary of the Organized Crime Situation Report 2004: Focus on the Threat of Cybercrime). http://download.springer.com/static/pdf/ (cited August 14, 2015).

18 ITU was founded in Paris in 1865 as the International Telegraph Union. It took its present name in 1934, and in 1947 became a specialized agency of the United Nations.

19 The ITU found that the percentage of Internet users among the whole population of Palestine is 46.6%.

have any officially recognised national or sector-specific program for sharing cybersecurity assets within the public sector. There is no officially recognised national or sector-specific program for sharing cybersecurity assets between the public and private sector. Furthermore, there is no information on any international cooperation Palestine participates in.[20]

The principle of *nullum crimen sine lege*[21] is fundamental to most legal systems worldwide.[22] Under this principle, any behaviour, no matter how harmful, cannot be prosecuted unless it is formally prohibited by law. However, some cybercrime offenses have gone unpunished in Palestine due to the lack of substantive legal provisions criminalizing such conduct. Palestinian public prosecutors and judges face major problems regarding prosecuting and judging cybercrimes because of the absence of comprehensive legislation that specifically addresses cybercrime. The Jordanian Criminal Code (JCC) of 1960, which is still applied in the West Bank,[23] lacks provisions to criminalize cybercrime. Indeed, the JCC clearly was enacted to protect physical objects. There is no Computer Crime Act, but there is a Draft Computer Transaction Law. Palestinian courts deal with the matter by using one of two approaches: In some instances, public prosecutors choose not to prosecute the act due to the fact that there is no provision of law applicable to the conduct. In others, they adapt the related conventional provisions of the JCC to the conduct. In such cases, however, some courts reject the interpretation and adaptation of the conventional provisions to the cybercrimes and consequently reject the case.

Evidence suggests that cybercrimes are committed daily in Palestine and may be increasing in frequency.[24] The Palestinian legislature and other decision makers appear, however, unaware of the danger Palestine will face in the future as a result of the size of cybercrime and prefer to write laws to counter the "more serious" crimes. They only think about cybercrime when bloggers

20 International Telecommunication Union (ITU), Cyberwellness Profile- State of Palestine. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Palestine%20.pdf (cited July 15, 2015).

21 No Crime and no Punishment without Law.

22 It means that the conduct (commission or omission) is not forbidden (criminalized) unless it is stated in the criminal law, or any other complementary penal law, that it is a crime and the law specifies a certain punishment for it.

23 The Territories under the rule of the Palestinian Authority (PA) consist of two areas: the West Bank which was under Jordanian Rule (1948–1967); and the Gaza Strip which was under the Egyptian Administration (1948–1967). The two areas are distinct geographically since 1948, but theoretically they are nowadays under the rule of the PA (since 1994). Gaza Strip shares most legislation with the West Bank, however the JCC is not applied there.

24 Statistics of cybercrime in Palestine are totally lacking.

insult the Palestinian regime and public officials.[25] Even in such cases, they try their best to find provisions in the JCC which can be adapted and applied. Although some experts argue that enacting new laws in Palestine is problematic nowadays because of the absence of the Legislative Council (Parliament),[26] and the fact that the President of the Palestinian Authority (PA) is reluctant to use his constitutional right to issue Presidential Orders. Others may argue that the PA can ratify and incorporate the Arab Convention on Combating Information Technology Offences of 2010 (hereinafter the Arab Convention on CITO)[27] in the domestic Palestinian legal system, especially that the PA joined the convention earlier. However, the legislative challenge is also the responsibility of the international community[28] since cybercrimes are borderless crimes. The lack of cybercrime legislation in one country can, directly or indirectly, influence the rest of the world by creating, for instance, jurisdictional havens.[29] But, in this concern the international community will face a problem. Palestine remains under occupation and has no control of its borders, therefore extradition of the accused and suspects will not be an easy task.

25 In September 2014 the Palestinian intelligence services arrested two journalists (26 and 22 year old men) in the West Bank, which is part of a broader pattern of monitoring and censoring social media activity, according to the Palestinian Center for Development and Media Freedoms (MADA). The first was "apprehended for insulting Fatah Central Committee member Azzam Al-Ahmad on his Facebook page and for accusing him of treason." The other one was "accused of defaming the public authority in journalistic posts he published on social networks and information websites such as Al-Quds and Wattan." https://electronicintifada.net/blogs/patrick-strickland/palestinian-authority-arrests-two-journalists-facebook-posts (cited July 25, 2015). Another recent case was on July 3rd, 2015, in which a 22 year old blogger wrote on his website at Facebook statements interpreted later as criticism against the head of the local council of his village regarding the bad services provided by the local council. The young man was arrested by the Civil Police and detained for five days, during which he was cruelly tortured. http://www.maannews.net/Content.aspx?id=792049 (cited August 13th, 2015).

26 The Palestinian Legislative Council did not convene since 2007 because of the civil war took place in Gaza Strip between Fatah and Hamas and the takeover of the Government in Gaza by Hamas militia.

27 Regional Convention enacted by the General Secretariat of the League of Arab States and ratified by eighteen Arab countries, including Palestine, on 21 December 2010. Although Palestine ratified the Convention, it did not translate it into its internal legislation.

28 The international community can play a vital role in this perspective through the different foreign and international institutions working in Palestine on different areas including the rule of law, empowering the judiciary and legislative development. They can develop their plans to include fighting and countering cybercrime.

29 Magaireh, supra note 5 at 38.

3 Scope and Methodology

Governments have various instruments to achieve policy goals. They build their policies and strategies with different measures to prevent crime. Many actions intended to address cybercrime and attain cybersecurity arise from technical protections by private actors. These include firewalls that prevent illegal access to a computer system, anti-virus software that can hinder the installation of malicious software, or filters that block access to illegal content.[30] Other actions focus on raising the capacity of consumers including raising awareness of ICTs users. Finally, some parties have engaged in international cooperation or developed novel legal instruments. This paper analyses current laws in light of the international standards and proposes relevant and effective reforms. Such legislation includes criminal laws, as well as appropriate regulations in related fields. The paper will focus in particular on a comparative approach to develop appropriate substantive criminal law which criminalizes cybercrime in Palestine.[31] Palestine needs legal reforms to address substantive and procedural criminal law, as well as jurisdictional issues,[32] but this paper will be limited to the substantive criminal law. Procedural issues such as search and seizure, jurisdiction, extradition, data interception, and methods of international cooperation will be addressed in a separate paper. This paper will examine the conventional provisions of existing Palestinian laws: the JCC and the Palestinian Telecommunication Law. It will then turn to the Council of Europe Convention on Cybercrime of 2001 (hereinafter the CoE Convention on Cybercrime[33]) and

30 Gercke, Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU Telecommunication Development Bureau. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (cited July 17, 2015).

31 The criminal procedures, which enable the Palestinian courts, public prosecution and law enforcement institutions to deal with cyber criminals efficiently, will be tackled in a separate article.

32 Buono, Laviero, supra, note 2.

33 The Convention on Cybercrime was drafted by the Council of Europe (COE) in Strasbourg, France. In addition to the CoE member states, Canada, Japan, South Africa and the United States of America participated in the negotiations of the Convention as observers. Forty-seven countries have signed the treaty. So far, only 36 countries have ratified it. Notable non-signatories include Russia, China, and several Latin American countries, all of which rank among the biggest sources of malicious code. The Convention consists of 48 articles in four chapters. It has an additional protocol on the criminalisation of acts of racist or xenophobic nature committed via the Internet.

the Arab Convention on CITO)[34] as points of departure for analysing future legislation. The relevant provisions of the Model Criminal Code (MCC)[35] and their commentaries will also be tackled. Furthermore, the Palestinian legal system will be compared with the Belgian one since Belgium was one of the first European countries which participated in drafting the CoE Convention on Cybercrime and also possesses developed cybercrime legislation.

The CoE Convention on Cybercrime seeks, among other goals, to address cybercrime by harmonizing national laws.[36] Furthermore, the drafters of the Convention aim to deter "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data".[37] That is to say, it aims to pursue a common criminal policy to combat and deter cybercrime, criminalize any conduct that constitutes a cybercrime, and facilitate detection, investigation and prosecution at both the domestic and international levels. Hence, the convention urges the States Parties to criminalize certain forms of conduct and harmonize their legal frameworks to combat cybercrime and facilitate international cooperation.[38] Meanwhile, the Arab Convention on CITO focuses on enhancing and strengthening cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals (article 1). The next section, and the focus of the paper, analyses individual existing Palestinian legislation

34 Regional Convention enacted by the General Secretariat of the League of Arab States and ratified by eighteen Arab countries, including Palestine, in 21 December 2010. Although Palestine ratified the Convention, it did not translate it into its internal legislation.

35 The Model Codes for Post-Conflict Criminal Justice Project was launched in 2001 by the United States Institute of Peace and the Irish Centre for Human Rights, in cooperation with the United Nations Office of the High Commissioner for Human Rights (OHCHR) and the United Nations Office on Drugs and Crime (UNODC). The MCC with its measured approach will enable jurisdictions emerging from conflict to move quickly toward re-establishing the rule of law and a fair criminal justice system, without the need to start the reform process afresh. See Vivienne O'Connor and Colette Rausch (ed.), Model Codes for Post-Conflict Criminal Justice, Volume I Model Criminal Code, United States Institute of Peace, Washington, D.C., 2008.

36 Portnoy, Michael and Seymour Goodman (Ed.), Global Initiatives to Secure Cyberspace, An Emerging Landscape. http://link.springer.com/book/10.1007/978-0-387-09764-0. (cited August 17, 2015).

37 Preamble of the Convention on Cybercrime.

38 Gercke, Marco, supra, note 14.

relating to specific cybercrimes in light of the CoE Convention on Cybercrime and the Arab Convention on CITO, and proposes reforms. Finally, the article summarizes key lessons from this analytical exercise.

4 Countering Cybercrime: Legislative Approach

Today, most nations are vulnerable to cybercrime. Whilst no single country has jurisdiction over cyberspace as a whole, regulating national cyberspace is possible.[39] It is therefore important to establish the necessary legal and institutional framework enabling prosecutions of these new and emerging forms of crime.[40] Palestine is no exception. Although it is one of the countries that has just entered the digital age, it may unwittingly serve as havens for computer criminals. Therefore, it is essential for the Palestinian Authority (PA) as well as the international community, to develop adequate legislation in this field. Suppose that a person situated in Palestine spread a dangerous virus[41] attacking specific or non-specific websites worldwide, this would be a danger for the international community.

The Palestinian legal context in 2016 resembles, to some extent, that of the Philippines before May 2000. At that time, the Philippines' competent institutions could not prosecute the person who released the "I LOVE YOU" virus because there was no law in that country which prohibited the release of malicious code.[42] The conduct attributed to de Guzman was a crime in the eyes of many countries, but not the Philippines. Despite billions of dollars of damage and hundreds of thousands of primary and secondary victims in dozens of countries, the individual responsible could not be brought to trial. No one has ever been prosecuted for the damage inflicted by the "Love Bug".[43]

39 United Nations Economic and Social Commission for Western Asia (UN-ESCWA), the ESCWA Cyber Legislation Digest. http://unctad.org/meetings/en/Contribution/CIIEM5_ESCWA_en.pdf (cited September 9th, 2015).

40 Grabosky, Peter, Requirements of prosecution services to deal with cybercrime. http://link.springer.com/article/10.1007/s10611-007-9069-1. (cited August 16, 2015).

41 Virus means: A computer program that may spread from computer to computer, as files containing the program are opened, using up available memory and degrading the "infected" systems and their networked computers.

42 Malicious Code means: Computer programs designed to cause damage to a computer or system; worms or viruses.

43 Goodman, Marc, supra, note 30 at 318–319.

In their description of cybercrime, two scholars Wall[44] and Grabosky,[45] tackled it from different points of view. Wall described it as "new wine, no bottles," meanwhile Grabosky described it as "old wine in new bottles." Some types of cybercrimes were committed in the past before the advent of the internet era, such as fraud, forgery, or child pornography. So, it does not all appear to be "new wine." Traditional crimes when committed using computer network "bottles" consist of well-worn elements and specifications, but the legislature might have to deal with them in a different way and inflict different penalties. Some scholars consider this way of dealing with cybercrimes, i.e. looking at them as digital versions of traditional offenses, as correct.[46] That is to say, many cybercrimes could be considered traditional or can be likened to traditional crimes. For instance, identity theft can occur in both physical and cyber arenas.[47] In contrast, some other experts do not consider such an application legal.[48] They think that it is not always right to apply provisions enacted to be applied outside the network to acts committed over the internet. Furthermore, they urge lawmakers to respond continuously to developments and monitor the effectiveness of existing legal approaches.[49] Lawmakers generally require a certain period of time to update national criminal law to enable the prosecution of new forms of cybercrime.[50]

The methodology used by nations to criminalise cybercrime varies. The required substantive law provisions can be incorporated into the criminal law or enacted through a separate cybercrime law. For example, in Finland cyber offences were regulated via new chapters of the penal code.[51] The Palestinian

44 Wall, D.S., Cybercrimes: New Wine, No Bottles? In Davies, P., Francis, P., Jupp, V. (eds.) Invisible Crimes: Their Victims and their Regulation. Macmillan, London (1999).

45 Grabosky, Peter, Virtual Criminality: Old Wine in New Bottles? Social and Legal Studies 10(2), 243–249 (2001).

46 Brenner, Susan, Thoughts, Witches and Crimes, CYB3RCRIM3: Observations on Technology, Law, and Lawlessness, May 6, 2009, http://cyb3rcrim3.blogspot.com/2009/05/thoughts-witches-and-crimes.html. (cited August 4th, 2015).

47 Finklea, Kristin and Catherine A. Theohary, Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, Congressional Research Service, January 15, 2015. http://fas.org/sgp/crs/misc/R42547.pdf. (cited September 10, 2015.

48 Arab, Younes, Computer Crime: Concept, Scope and Peculiarities, Arab Centre for Criminal Studies, Abu Dhabi, 2002.

49 Gercke, Marco, Europe's Legal Approaches to Cybercrime, ERA. http://link.springer.com/article/10.1007/s12027-009-0132-5. (cited August 15, 2015).

50 Marco Gerke, supra note 49.

51 Makela, Liisa, supra note 7.

legislature may not be capable of enacting new chapters of the criminal code under the current situation (i.e., in the absence of the Legislative Council (Parliament)), but this should be the long term goal. In the short term, however, the President of the PA has the constitutional authority to review and update the JCC via Presidential Order. Among other amendments, he can, for example, give digital information an equivalent legal status to traditional signatures and printouts. Palestine must work hard, like many other countries,[52] to make legislative adjustments to keep up with technical changes.

5 Developing Draft Palestinian Substantive Cybercrime Provisions

There are many classifications of cybercrime.[53] Some scholars have classified them into five, others into four, three and two. In this paper, the classification of the CoE Convention on Cybercrime will be mainly adopted, since its classification is more comprehensive and logical. Furthermore, forty-seven countries have signed the treaty, including CoE Member States, Canada, Japan, South Africa and the United States of America. The CoE Convention on Cybercrime contains nine criminal offenses in four different categories: (1) offenses against the confidentiality, integrity, and availability of computer data and systems; (2) computer related offenses; (3) content related offenses; and (4) offenses related to the infringement of copyright and related rights. The CoE Convention on Cybercrime does not include some other crimes which are facilitated using the computer, such as money laundering, identity theft, and storing illegal data.[54] Meanwhile, the Arab Convention on CITO tackled offences related to organized crime committed by means of information technology, including: money-laundering operations, assistance or disseminating money-laundering methods; advocate the use of and traffic in drugs and Psychotropic Substances; traffic in persons; traffic in human organs; and illicit traffic in arms (Article 16).

5.1 *Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems*

Here we will analyse the following cybercrimes respectively: illegal access; illegal interception; data interference; system interference and misuse of devices.

52 Marco Gerke, supra note 49.

53 For example, the UN Manual on the Prevention and Control of Computer-related Crime (1999).

54 Alkaabi (et al.), supra note 8 at 3.

5.1.1 Illegal Access to a Computer System

Illegal or unlawful[55] access to a computer system is described in jurisprudence as "hacking",[56] "cracking",[57] or "computer trespass".[58] It covers the "basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data.[59] It "comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data)".[60] "Examples of hacking offences include breaking the password of password- protected websites and circumventing password protection on a computer system, setting up "spoofing" websites to make users disclose their passwords and installing hardware and software-based keylogging methods (e.g. "keyloggers") that record every keystroke- and consequently any passwords used on the computer and/or device".[61]

Among the targets of hacking attacks are the US Department of State (Wiki Leaks), US Air Force, the Pentagon, Yahoo, Google, E-bay, etc. The motivations of the "hackers" vary according to many factors. Some offenders access a computer system in order to prove their abilities in ICTs; others are politically oriented; meanwhile most offenders, including the most dangerous, are those who benefit from legal access to commit further crimes by obtaining passwords to commit data espionage; data manipulation; or distributed denial of service attacks (DDoS).[62]

The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response also has to include the threat and use of criminal law measures. A criminal prohibition of unauthorised access provides additional

55 Gercke, Marco, supra note 49.

56 Hacking means: obtaining unauthorized access to a computer.

57 Cracking means the defeating of security devices in computer networks.

58 A person is guilty of computer trespass if s/he intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer network, computer program, or data. Computer trespass is directed generally towards computer hackers.

59 The Explanatory Report of the CoE Convention on Cybercrime (Note 44).

60 The Explanatory Report of the CoE Convention on Cybercrime (Note 46).

61 Gercke, Marco, supra note 49.

62 Distributed Denial of Service (DDoS) Attack means: an individual (usually a hacker) gains remote access to a number of computers and directs them against a target (usually a computer system belonging to a government or large commercial entity). By overloading the target computer, the attack will impede legitimate access and may render the system inoperable.

protection to the system and the data as such as well as providing early protection against the dangers described above. It is among the measures the CoE Convention on Cybercrime urges State Parties to the convention to adopt.[63] Thus, criminal prohibition of illegal access is important to combat cybercrime by giving additional protection against threats to the system and data, especially as illegal access "may lead to impediments to legitimate users of systems and data and may give access to confidential data (including passwords, information about the targeted system) and secrets".[64]

The elements of the crime of "illegal access", according to the CoE Convention on Cybercrime are:

1 The conduct: the access to the whole or any part of a computer system, such as the access of a web page, directly or through hypertext links, including deep-links or the application of 'cookies' or 'bots'[65] to locate and retrieve information on behalf of communication;[66]
2 The lack of excuses, or "without right":[67] the access is not authorised by the owner of the system (e.g. for testing or protection of the computer system concerned or for "accessing a computer system[68] that permits free and open access by the public, as such access is "with right";[69] and
3 The consent: the act is committed intentionally.

The Arab Convention on CITO criminalizes the illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. Meanwhile, the convention aggravates the punishment if the conduct (i.e., access, presence, contact or perpetuation) leads to: a- the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damage to the users and beneficiaries; or b- the acquirement of secret government information (article 6).

63 Article 2 of the CoE Convention on Cybercrime. See also the preamble of the Convention.
64 The Explanatory Report of the CoE Convention on Cybercrime (Note 45).
65 "Bot" (abbreviation of robot) means: a computer program that runs automatically. Some bots have beneficial uses, but others may be employed to gain unauthorised control over a target's computer.
66 The Explanatory Report of the CoE Convention on Cybercrime (Note 48).
67 Paragraph 38 of the explanatory report to the CoE Convention on Cybercrime discusses the meaning of "without right".
68 For a discussion of the meaning of computer system, reference should be made to paragraphs 23–24 of the Explanatory Report of the CoE Convention on Cybercrime.
69 The Explanatory Report of the CoE Convention on Cybercrime (Note 47).

The Palestinian legislation does not explicitly contain provisions on "hacking" offences, but the Basic Law (amended) of 2003 implies protection from such offences when it stresses the protection of human rights.[70] Furthermore, it clarifies that "any violation of any personal freedom, of the sanctity of the private life of human beings, or of any of the rights or liberties that have been guaranteed by law or by this Basic Law shall be considered a crime…"[71]

The Telecommunication Law of 1996 also tackles the issue in broad and vague provisions. It states that the privacy of telecommunications is maintained, and there is no person or entity entitled to infringe such privacy but the public authority according to law.[72] The Criminal Procedures Code (CPC) specifies the conditions and mechanism of such interference by the public prosecuting authorities, in the private life of people, including surveillance of telephone calls.[73] On the other hand, some scholars draw an analogy between illegal access to a computer and illegal access to a house.[74] Although the legislature has similar goals in the two cases represented for the protection of the privacy of people, this analogy is not accurate (according to the JCC at least) for many reasons: first, the access to the house is physical, while the access to the computer system is virtual, i.e. the provision enacted to protect the privacy of the house is targeting a physical object; second, the access to the house may have aggravating circumstances when committed during the night or using violence or committed by two or more people, but it's not the same when the illegal access to computer system occurs with one or other of the abovementioned circumstances; third, the prosecution of the illegal access to a house may not take place without the complaint of the victim, whereas the cybercrime maybe prosecuted without complaint. We conclude through this analysis that the abovementioned provisions of the JCC are insufficient to combat the offense of illegal access to computer systems.

The proposed Palestinian cybercrime code should differentiate between external and internal hacking by the levels of severity of punishment. External

70 Article 10 of the Basic Law states that: "1. Basic human rights and liberties shall be protected and respected. 2. The Palestinian National Authority shall work without delay to become a party to regional and international declarations and covenants that protect human rights."

71 Article 32 of the Basic Law (amended), published in a special volume of the Palestinian Official Gazette on March 19th, 2003.

72 Article 4 of the Telecommunication Law, published in volume no. 12 of the Palestinian Official Gazette on April 23rd, 1996.

73 Article 51 of the Criminal Procedures Law, published in volume no. 38 of the Palestinian Official Gazette on September 5th, 2001.

74 Sai'ed, Kamel, Computer Crime, *Dar Al Thaqafeh*, Amman-Jordan (1994).

hacking, which is committed from outside the system is less severe, according to the Belgian Computer Crime Act, than internal hacking, which is committed from inside the system. Using the same comparative law, the attempt or inciting others to commit the offence and receiving the hacked data where the perpetrator knows its nature, are punishable. All punishments are doubled when they are repeat offences.[75]

5.1.2 Illegal Interception

Interception includes taking knowledge of, listening to, monitoring or surveillance of the content of communications, or recording them. The act of keeping, disclosing, distributing, and using the content of illegally intercepted communications also qualifies as interception. Interception may be conducted by fixing technical devices to transmission lines as well as devices to collect and record wireless communications. It may include the use of software, passwords and codes.[76]

As the illegal access to computer systems is considered a crime in most countries worldwide, because it is considered a violation of the constitutional right to privacy, the illegal interception of data is a crime too. It is also enshrined in international human rights instruments.[77] The offence of illegal interception applies the principle of privacy to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.[78] The Convention on Cybercrime urges the legislatures of the State Parties to criminalize any attack against the privacy of computer data, when the interception is committed by technical

75 Paul De Hert, and Boulet Gertjan (2013) Cybercrime report for Belgium: national report for the first Preparatory Colloquium on "Criminal Law, General Part" (Verona, Italy, 28 30 November 2012) for the 19th International Congress of Penal Law on "Information Society and Penal La. International Review of Penal Law (RIDP / IRPL), issue 84, vol.2013, n. 1–2, pp. 12–59. http://www.penal.org/IMG/pdf/RIDP_2013_1_2_CD_Annexe.pdf

76 The Explanatory Report of the CoE Convention on Cybercrime (Note 53).

77 Article (17) of the International Covenant on Civil and Political Rights states that: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks". Also article (8) of the European Convention on Human Rights states that: "1. everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

78 The Explanatory Report of the CoE Convention on Cybercrime (Note 51).

means, intentionally and without right.[79] Article 7 of the Arab Convention on CITO also criminalizes the deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data. Illegal interception represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he/she acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities.[80] The offence of illegal interception according to the Palestinian legislation is committed by any person, including public officials, when they exceed their legal authority to wiretap a communication or a telephone call. As is evident from the relevant Palestinian legal provisions,[81] the legislature intended to

79 Article 3 of the CoE Convention on Cybercrime.

80 The Explanatory Report of the CoE Convention on Cybercrime (Note 58).

81 Article (356) of the JCC (published in volume no. 1437 of the Jordanian Official Gazette on May 1st, 1960) states that: "Each public servant works for any post office who abuses his/her function through opening the envelope of a message or crashing or skimming a message or sending it to another person (not the addressee) shall be punished by imprisonment of one month to one year. He/she shall be punished with imprisonment of six months or a fine of up to 20 Jordanian Dinars (JD) each public servant works for the Department of Telecommunication if he/she discloses a telephone call knew about it by virtue of his/her job". Meanwhile, article (357) of the JCC states that: "Every person who destroys or intentionally reads a letter or telegram not sent to him shall be punished by fine not exceeding five JD", whereas article (379) of the JCC states that: "Anybody who intentionally cuts a telephone call either through making damage to the machinery or wire or in any other manner, shall be punished by imprisonment from three months to two years. If the act leads to a real danger to public safety, the punishment shall be imprisonment from six months to two years".

On the other hand, article (51) of the CPC states that: "The Attorney General or one of his assistants may seize letters, communications, newspapers, printed matter, parcels and telegrams at post and telegraph offices when such relate to the crime and its perpetrator. He may also tap telephone and wireless communications and record conversations in private places on the basis of an authorization from the conciliation judge when such is useful in revealing the truth in a felony or a misdemeanor punishable by imprisonment for a term of not less than one year. The search warrant or the tapping or recording authorization must be reasonable and remains in force for a period of not more than fifteen days, subject to renewal once".

protect the use of telecommunication services, but there is a need for the legislature to intervene to criminalize the illegal interception of phone conversations and determine an appropriate penalty. The legislature is also invited to evaluate to what extent similar protection is offered to IP-based services.[82]

Of course, the interception becomes legal with the consent of all the participants of the communication. However, the Belgian Supreme Court has also considered that where one person records a telephone call in which they participate, that is not a crime. The court accepted the call recording as evidence delivered by the plaintiff in the criminal case as long as the call was initiated by the defendant who threatened the plaintiff over the phone.[83] The Belgian legislature introduced a provision to the Criminal Code prohibiting any interception of telephone calls or emails and other means of communications performed by employers of their employees. The article states that "except with the consent of all other persons directly or indirectly concerned by the information, identification of data given hereinafter, a person may not, himself or via a third party examine, with fraudulent intent, the existence or content of characters, signs, documents, images, sounds or data of any nature transferred by telecommunications originating from and intended for other persons' or examine, with intent, telecommunications data relating to another person".[84]

5.1.3 Data Interference

The protected legal interest in this offence is the integrity and the proper functioning or use of stored computer data or computer programs.[85] The CoE Convention on Cybercrime urges the State Parties to protect computer data by criminalizing any damage, deletion, deterioration, alteration or suppression of computer data when it is committed intentionally and without right.[86] The report of the CoE Convention on Cybercrime gave accurate definitions of the terms used. It states that the acts 'damaging' and 'deteriorating' relate in particular to a negative alteration of the integrity or of information content of

82 Gercke, Marco, supra note 49.

83 The Belgian Supreme Court, issued on January 9th, 2001. Located at http://www.lexadin.nl/wlg/courts/nofr/eur/lxctbel.htm (last modified July 28th, 2015).

84 The Law of June 30th, 1994 concerning the Protection of Privacy. Located at http://www.wipo.int/wipolex/en/details.jsp?id=403.

85 The Explanatory Report of the CoE Convention on Cybercrime (Note 60).

86 Article 4 of the CoE Convention on Cybercrime states that: "1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm".

data and programmes. The term 'alteration' means the modification of existing data. It considers the act 'deletion' of data as the equivalent of the destruction of a corporeal thing. Meanwhile, 'suppressing' of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. It considers the input of malicious codes, such as viruses and Trojan horses,[87] as the resulting modification of the data.[88] Meanwhile, article 8 of the Arab Convention on CITO considers the deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data as an offence against the integrity of data. But, the convention stipulates that in order to criminalize such acts mentioned above, they must cause severe damage. On the other hand, the JCC criminalises the destruction of movable properties.[89] The law aims to protect the movable (tangible) properties. Despite that, some judges and scholars may argue that the article is applicable to the conduct of data interference.[90]

Given the abovementioned definitions, this author considers that the conventional provisions of both the JCC and the CPC may be applicable to computer data since the aim of the CoE Convention on Cybercrime is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage.[91]

5.1.4 System Interference

System interference means the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. This conduct becomes a crime when it is committed intentionally. The CoE Convention on Cybercrime urges the State Parties to criminalize any act which constitutes computer sabotage.

87 Trojan Horse means: a malicious program disguised as legitimate software but which, when transmitted to an unsuspecting recipient, may impede functioning of the target computer system, and may even facilitate unauthorized access and control over one's computer.

88 The Explanatory Report of the CoE Convention on Cybercrime (Note 61).

89 Article (445) of the JCC states that "Anyone who causes damage, intentionally, to the movable properties of other(s) shall be punished, on the basis of a complaint lodged by the aggrieved party, by imprisonment not exceeding one year or a fine not exceeding 50 dinars or both".

90 Said, Kamel, supra note 74.

91 The Explanatory Report of the CoE Convention on Cybercrime (Note 60).

The term 'hindering' refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data.[92] Furthermore the hindering must be "serious" in order to give rise to criminal sanction. The drafters of the CoE Convention on Cybercrime considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system.)[93] In the opinion of the drafters, the conduct of sending spam[94] should only be criminalised where the communication is intentionally and seriously hindered.[95]

The Palestinian legislation is still silent concerning the infringement of computer systems. In the meantime the Telecommunication Law criminalises the act of hampering or deletion of the content of a letter by telecommunication networks or encouraging others to do so. Although this provision is not ideal, it might be adapted and applied until a cybercrime law is enacted. However, the punishment the legislature determined for this offence is light (either imprisonment for not less than one month and not more than six months, or a fine of not less than 50 and not exceeding 200 JD, or both).[96]

5.1.5 Misuse of Devices

The misuse of device refers to "the intentional commission of specific illegal acts regarding certain devices (such as "hacker tools") or access data to be misused for the purpose of committing either the production, sale, procurement for use, import, distribution or otherwise making available of a device or a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed".[97] The report of the CoE Convention on Cybercrime clarified some terms and expressions. Among

92 The Explanatory Report of the CoE Convention on Cybercrime (Note 66).

93 The Explanatory Report of the CoE Convention on Cybercrime (Note 67).

94 Spam means: unsolicited electronic mail, often transmitted in large volume, whether for legitimate commercial purposes or in furtherance of fraud.

95 The Explanatory Report of the Convention on Cybercrime (Note 69).

96 Article 92 of the Telecommunication Law.

97 Article 6 paragraph 1 of the CoE Convention on Cybercrime. See also the Explanatory Report of the CoE Convention on Cybercrime (Note 70).

others, the term 'distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing of online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a 'computer program' refers to programs that are, for example, designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.[98] **The Arab Convention on CITO tackled the offence of misuse of information technology by designating it as means of the production, sale, purchase, import, distribution or provision of any tools or programmes designed or adapted for the purpose of committing the computer offences; or the information system password, access code or similar information that allows access to the information system with the aim of using it for any of the computer offences (Article 9).**

The question which may arise is whether the tools and devices referred to in the laws discussed are meant to be restricted just to those which are designed exclusively for committing offences, or are meant to include all tools and devices? In fact, neither of the two extremes was preferred by the drafters of the CoE Convention on Cybercrime, since the first would lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances and the second was also rejected because many tools and devices can be used to commit crimes, for example knives, swords, and machine guns. The decisive criterion which determines whether producing and distributing the tool and device is legal or illegal, according to the drafters, depends on the subjective element of the intent of committing a computer offence.[99] In this sense, the Palestinian legislation lacks any provision criminalising the misuse of tools and devices. The legislature is therefore invited to intervene to counter such an offence.

5.2 *Computer-Related Offences*

Hereinafter, three offences will be tackled as examples of computer-related offences, namely: computer-related forgery; computer-related fraud and identity theft.

5.2.1 Computer-Related Forgery

According to the CoE Convention on Cybercrime, computer-related forgery means any addition, alteration, deletion, or suppression of computer data,

98 The Explanatory Report of the CoE Convention on Cybercrime (Note 72).

99 The Explanatory Report of the CoE Convention on Cybercrime (Note 73).

which results in inauthentic data, with the intent of using it as if it were authentic.[100] In this regard, alteration means any modification, variation, or partial changes of data. Deletion means any removal of data from a data medium. Meanwhile, suppression means holding back or concealment of data. It is expressly stated in the Report of the CoE Convention on Cybercrime that forgery is committed whether the addition (input) was of "correct or incorrect data".[101] The Arab Convention on CITO defines the forgery offense as the use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data (article 10). Furthermore, it tackled the illicit use of electronic payment tools in one of the following ways: any person who forges, manufactures or sets up any instrument or materials that assist in the forgery or imitation of any electronic payment tool by whatever means; any person who takes possession of the data of an electronic payment tool and uses it, gives it to a third party or facilitates its acquisition by a third party; any person who uses the information network or an information technology means to unlawfully access the numbers or data of a payment tool; or any person who knowingly accepts a forged payment tool (Article 18).

According to a specialist in cybercrime, cyber forgery can be defined as "any misrepresentations produced via computer, whether generated to a hard copy such as in making counterfeit money or submitted electronically using fraudulently obtained credit or credentials". Or "the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offense of forgery if it had been committed with respect to a traditional object of such an offence".[102] According to the abovementioned definitions, cyber forgery takes two forms: first, the use of computer systems to forge computer copies of physical records, such as passports and certificates (traditionally, a signature proves the authenticity of a document). Second, it is the use of computer systems to forge electronic or software dependent records, such as e-mails, and bank account statements. In that sense, computer-related forgery describes the manipulation of digital documents. This offence can be committed by creating a document that appears to originate from a reliable institution, manipulating electronic images (for example, pictures used as evidence in court) or altering text documents. The falsification of e-mails (cyber forgery) is an essential element

100 Article 7 of the CoE Convention on Cybercrime.

101 The Explanatory Report of the CoE Convention on Cybercrime (Note 83).

102 Maghaireh, supra note 3 at 63–64.

of phishing,[103] which seeks to make targets (victims) disclose personal/secret information. Often, offenders send out e-mails that look like communications from legitimate financial institutions. The e-mails are designed in a way that makes it difficult for targets to identify them as fake e-mails. The e-mail asks recipients to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers etc.[104]

Although criminal codes worldwide contain provisions which are applied to acts of forgery related to tangible documents, article (7) of the CoE Convention on Cybercrime criminalizes the forgery of intangible documents, i.e. stored electronic data. There is no doubt that the conventional provisions of most local criminal codes are not applicable to acts of forgery related to intangible documents, since electronic data is different from the data contained in tangible documents. Therefore, it is essential to plug the gaps in this area.

To answer the question whether or not the JCC criminalizes cyber forgery; there is no explicit answer in its provisions, nor does the JCC define 'document'. Therefore, we have to analyse the relevant provisions in order to give the right answer. As mentioned earlier, there are two types of forged documents (whether formal or informal), the first one is physical in form (the computer printouts) such as an identity card or a birth certificate forged using a computer and printed and submitted; and the second is an electronic or software version. We can simply conclude that forging the first type of documents is a crime under the JCC; meanwhile forging the second type (the electronic documents) is not a crime under the same law because the JCC does not protect intangible documents, i.e. there is no single provision which deals with intangible things except for electricity in the crime of theft;[105] secondly the JCC does not

103 Phishing means: transmitting a form of Spam containing links to Web pages that are designed to appear to be legitimate commercial sites. They seek to fool users into submitting personal, financial or password data. Clicking on the link may also lead to infection of one's computer by a virus, or may allow access to one's computer by a hacker. Phishing describes attempts to fraudulently acquire personal, secret or sensitive information (passwords, usernames, credit cards details, account numbers, etc.). Very often this is done by copying websites ("spoofing website"). See Gercke [1], p. 606. See also information and statistics offered by the anti-phishing working group, which is available at: www.antiphishing.com (cited July 25th, 2015).

104 Gercke, Marco, supra note 14.

105 Article 399 paragraph 2 of the JCC states that "the word "money" includes the forces which could be acquired". Commentators in their illustration of the abovementioned article clarify that the acquired forces include electricity despite it not being tangible. See Sa'ied, Kamel, supra note 74.

recognize digital records (such as disks and tapes) as documents. However, the Draft Electronic Transaction Law criminalizes forging any electronic signature (article 49), and criminalizes any forgery of an electronic document (formal or informal) (article 52). In any event, there are no cyber forgery cases which have been tried before the Palestinian courts as yet, or more accurately, no judgments have yet been rendered by the Court of Cassation in this regard.[106] However, we can expect, through analogy with other related matters, that the judges will apply the JCC to such acts, i.e. they will criminalise cyber forgery by applying the traditional provisions applicable to tangible documents.

The report on the CoE Convention of Cybercrime stipulated that the forgery of computer-related data may not be committed unless a third party is misled.[107] This is different from the domestic law applied in Palestine, for example, where forgery is considered to have been committed whether a tort has occurred or not. According to the JCC, forgery is an intentional distortion or modification of truth in an authentic document or data resulting in damage or which may result in damage, whether the damage was physical, moral or social.[108] The perpetrator shall be punished with the same penalty for forgery if he/she used a forged document only if he/she knows that the document is forged, unless the law specifies a special penalty.[109] Under Belgian law, the use of forged computer data is an autonomous crime. No special intent is required. One only needs to have known that the data was false. On November 28th, 2005, the Criminal Court of Dendermonde found that creating an e-mail account in the name of someone else and sending an e-mail from this account to another person constitutes computer forgery.[110]

The forgery crime in domestic laws is committed either through denying or deceiving someone as to the authenticity of the author of the document "regardless of the correctness or veracity of the contents of the data", or "based on the truthfulness of the statement contained in the document".[111] Also, the act is considered forgery either when it is committed against a "public document" or a "private document, which has legal effect",[112] or, as stated in the Palestinian legislation, against "a formal document or informal one".[113]

106 The High Judicial Council publishes the judgments of the Court of Cassation only.

107 The Explanatory Report of the Convention on Cybercrime (Note 81).

108 Article 260 of the JCC.

109 Article 261 of the JCC.

110 Paul De Hert, supra note 75 at p.898.

111 The Explanatory Report of the CoE Convention on Cybercrime (Note 82).

112 The Explanatory Report of the CoE Convention on Cybercrime (Note 82).

113 Article 271 of the JCC.

According to the MCC, any person is considered a perpetrator of the criminal offense of forgery under the following two conditions: when he/she makes a false instrument with the intention that he/she or another person will use it to induce another to accept it as genuine; and when he/she accepts the false instrument to gain something or to cause loss.[114] The MCC considers that the "instrument" includes, but is not limited to the following: disc, tape, soundtrack, or other device on or in which information is recorded or stored by mechanical, electronic, or other means; money orders; postage stamps; official licenses or stamps issued by the state; checks, including travellers' checks and bank drafts; credit cards, debit cards, or other charge cards; share certificates; and passports or other documents that can be used instead of a passport.[115]

The MCC states that this article does not apply if the act is counterfeiting money, since another provision of the MCC will be applied. The MCC does not differentiate between whether the instrument was of an informal or formal character. Contrary to the MCC and the JCC, the CoE Convention on Cybercrime does not tackle the two related crimes of forgery, namely "using false instruments" and "possessing false instruments". The MCC defines the act of using false instruments as "a person commits the criminal offense of using false instruments when he or she uses a false instrument, knowing that it is false: (a) with the intention to induce another to accept it as genuine; and (b) by reason of so accepting it, to obtain a gain or cause a loss".[116] Whereas, it defines the act of possessing false instruments as: "a person commits the criminal offense of possession of false instruments when he or she has in his or her possession a false instrument, knowing that it is false: (a) with the intention that that person or another will use it to induce another to accept it as genuine; and (b) by reason of so accepting it, to obtain a gain or cause a loss".[117]

5.2.2 Computer-Related Fraud

Conventional fraud can be defined as manoeuvres that damage the intent of persons in order to deceive them into giving their money to the criminal.[118] Meanwhile, computer-related fraud concerns interference of a machine. It can be defined as "the gaining for oneself or another, a fraudulent profit through entering, changing, deleting or in any other way altering the potential use of

114 Article 128 paragraph 1 of the MCC.

115 Article 128 paragraph 2 of the MCC.

116 Article 129 of the MCC.

117 Article 130 of the MCC.

118 Article 417 of the JCC.

computer data in a computer system".[119] Thus, the main distinction between computer-related fraud and traditional fraud is the target of the fraud. If the offender tries to influence a person, the offence is generally recognized as fraud. Where the offender targets computer or data- processing systems, the offence is often categorized as computer-related fraud. Examples of computer-related fraud are the use of a stolen credit card to withdraw money from an JCC, exceeding the limit of one's own credit card without authorisation and manipulating of bank accounts by a bank employee.[120] Computer-related fraud, according to the CoE Convention on Cybercrime, may be committed by any input, alteration, or suppression of computer data for the aim of gaining an economic benefit for oneself or for another person. Some scholars argue that article (8) of the CoE Convention on Cybercrime does not stipulate acquiring financial gain as a constituent element of the crime, but it is enough to act with the intention of gaining something.[121] Of course, the act may not be considered criminally fraudulent unless it is committed intentionally, without right, and causes the loss of property to another person.

Meanwhile, the Arab Convention on CITO defines computer-related fraud as any conduct intentionally and unlawfully causing harm to beneficiaries and users with the aim of committing fraud to illicitly realize interests and benefits to the perpetrator or a third party, through:

1 entering, modifying, obliterating or concealing information and data.
2 interfering with the functioning of the operating systems and communication systems, or attempting to disrupt or change them.
3 disrupting electronic instruments, programmes and sites (article 11).

The target of computer-related fraud may be represented in electronic funds and deposit money. The crime is mainly committed by feeding the computer with incorrect data.[122] Computer-related fraud manipulations are criminalised if they produce a direct economic loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person. The term 'loss of property', being a broad notion, includes loss of money, tangibles and intangibles with an economic value.[123]According to the MCC, a person commits the criminal offense of fraud

119 Paul De Hert, *supra note 75*, at 896.
120 Paul De Hert, *Ibid*, p. 896.
121 Paul De Hert, *Ibid*, p. 896.
122 The Explanatory Report of the CoE Convention on Cybercrime (Note 86).
123 The Explanatory Report of the CoE Convention on Cybercrime (Note 86).

when he or she is involved in the following acts: making unlawful material gain for himself or herself or for another person or causing loss to another person; inducing another person by deception to do or refrain from doing an act to the detriment of his or her property or the property of another.[124] The property here includes movable property, whether tangible or intangible, in addition to immovable, intangible property.[125]

Nowadays, the most common computer-related fraud offences include online auction fraud and advanced fee fraud.[126] The online auction fraud may be committed either through offering non-existent goods for sale and requesting buyers to pay prior to delivery and buying goods and asking for delivery, with no intention of paying. In response, auction providers have developed protection systems such as the feedback/comments system. After each transaction, buyers and sellers leave feedback for use by other users as neutral information about the reliability of sellers/buyers. In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to pay for non-existent goods. The second method involves sending out goods without receiving payment first. However, criminals have responded and circumvented this protection by using accounts from third parties. In this scam called "account takeover", offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult".[127]

In advance fee fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts. The offenders then ask them to transfer a small amount to validate their Iban account data (based on a similar perception as lotteries- respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just to send bank account data directly. Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities. Evidence suggests that thousands of targets reply to such fraudulent e-mails.[128]

124 Article 126 paragraph 1 of the MCC.

125 Article 119.1(2) of the MCC.

126 Gercke, Marco, supra note 5.

127 Gercke, Marco, supra note 14.

128 Gercke, Marco, *Ibid.*

The criminal law systems that cover traditional fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the abovementioned offences. Thus, article (417)[129] of the JCC can be applied to acts which constitute computer-related fraud since the method of committing the crime is not important. However, these provisions are inadequate and do not suit the computer and internet spheres, especially in relation to the massive loss and harm that may be caused by the computer-related fraud which needs harsher penalties, but until the enactment of proper new provisions, the conventional ones may be applied.

5.2.3 Identity Theft

Online identity theft or obtaining the others' personal information through the internet with the intent of fraudulently reusing it for criminal purposes is now one of the main threats to e-business.[130] Identity theft can be defined as "the criminal act of fraudulently obtaining and using another person's identity".[131] Identity theft differs from traditional theft, among other things the latter targets tangible movable objects whereas the first targets intangible things. If we try to draw an analogy with the traditional crime of theft, the latter requires that an object be physically removed, with the intention of permanently depriving the owner of that object.[132] However, technology nowadays allows for the perfect reproduction of texts, images, sound, video, and multimedia combinations whilst leaving the originals in place.

Therefore, when applying the traditional theft provisions of the JCC to identity theft, the legality principle hinders an interpretation of the offence of theft in a way which extends it to cover the theft of another person's identity. A person's identity is not a movable property that can be stolen from the possession of another. Identity theft has no essential element of offence described in law.[133]

Thus, the Palestinian legislature has to broaden the law of traditional theft, as well as criminal damage.

---

129 Article 417 of the JCC states that anybody deceived by someone else into transferring to him/her or to a third party money or undertaking using fraudulent means or disposal of movable or immovable money knowing that he has no right to such disposal or taking a false name or incorrect identity shall be punished by imprisonment from three months to three years and a fine from five to 50 JD.

130 Gercke, Marco, supra note 14.

131 Gercke, Marco, *Ibid.*

132 Article 399 of the JCC.

133 Makela, Liisa, supra note 7.

5.3 *Content-related Offences*

Two content-related offences will be tackled here, namely offences related to pornography (including child pornography); and religious, press and hate speech offences.

5.3.1 Offences Related to Pornography (including Child Pornography)

Child pornography means "any representation by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes",[134] whereas cyber pornography means "the use of cyberspace to disseminate pornographic materials".[135] Adult pornography is not prohibited in most countries. That is to say, "different countries criminalize erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors access this kind of material, seeking to protect minors. Other countries criminalize any exchange of pornographic material even among adults, without focusing on specific groups (such as minors)".[136]

However, the issue of pornography is not dealt with under the CoE Convention on Cybercrime nor under the MCC,[137] except as it relates to child pornography. Therefore, the CoE Convention on Cybercrime and the MCC only criminalize child[138] pornography. The ban on child pornography comes as a response to the international efforts to fight this phenomenon, and as a result of the "adoption of the Optional Protocol to the UN Convention on the Rights of the Child, on the Sale of Children, Child Prostitution and Child Pornography and the European Commission initiative on combating sexual exploitation of children and child pornography (COM2000/854).[139] According to the CoE Convention on Cybercrime and the MCC the following acts when committed intentionally and without right constitute cyber child pornography: producing

134 Article 118 of the MCC.

135 Maghaireh, supra note 5, p. 67.

136 Gercke, Marco, supra note 14.

137 The wording of paragraph 1 of Article 117 of the MCC is derived from Article 3(1)(c) of the Optional Protocol to the Convention on the Rights of the Child, on the Sale of Children, Child Prostitution and Child Pornography whereas the wording of paragraph 2 of article 117 comes from Article 9(1) of the CoE Convention on Cybercrime, and it covers child pornography perpetrated through the medium of computers.

138 The term "child" or "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall not be less than 16 years.

139 The Explanatory Report of the CoE Convention on Cybercrime (Note 92).

child pornography for the purpose of its distribution[140] through a computer system; offering[141] or making available[142] child pornography through a computer system; distributing or transmitting child pornography through a computer system; procuring[143] child pornography through a computer system for oneself or for another person; possessing[144] child pornography in a computer system or on a computer-data storage medium.[145]

According to the Arab Convention on CITO, the following conducts constitute the offence of pornography: the production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that constitutes outrage of modesty through information technology. The punishment shall be increased for offences related to children and minors pornography. The aggravated penalty also covers the acquisition of children and minors pornographic material or children and minors material that constitutes outrage of modesty, through information technology or a storage medium for such technology (article 12). The Convention also mentions other offences related to pornography, including gambling and sexual exploitation (article 13).

It is noted that the CoE Convention on Cybercrime considered the possession of child pornography an act which is equal in severity to the other acts constituting the offence such as producing, offering, distributing, and procuring child pornography. This approach is different from that adopted by the drafters of the MCC which placed the possession of child pornography in a separate provision and determined a different penalty range for it from the

140 'Distribution' is the active dissemination of the material. Sending child pornography through a computer system to another person would be addressed by the offence of 'transmitting' child pornography. The Explanatory Report of the CoE Convention on Cybercrime (Note 96).

141 'Offering' is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it.

142 'Making available' is intended to cover the placing of child pornography online for the use of others e.g. by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography." (The Explanatory Report of the CoE Convention on Cybercrime (Note 95).

143 The term 'procuring for oneself or for another' means actively obtaining child pornography, e.g. by downloading it. (The Explanatory Report of the CoE Convention on Cybercrime (Note 97).

144 "The possession of child pornography stimulates demand for such material. An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession." (The Explanatory Report of the CoE Convention on Cybercrime (Note 98).

145 Article 7 of the CoE Convention on Cybercrime.

offenses that involve the making or distribution of child pornography offenses because it is considered less serious and consequently subject to a lighter penalty range.[146] The criminal offense of possession[147] of child pornography includes possessing child pornography in a computer system or on a computer data-storage medium.[148]

Concerning child online protection in Palestine, there is no specific legislation. Palestine has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Palestine has acceded, with no declarations or reservations to article 2 and 3, to the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. There is no agency responsible for child online protection in Palestine. Concerning the reporting mechanism, there is no website or hotline dedicated to child online protection in Palestine.[149] Although the JCC prohibits and criminalizes the publication of offensive materials anywhere (even on the internet since the rule is wide enough to cover every single place considered as a crime scene),[150] there are a tremendous number of porn websites on the internet, which are available to everybody and the Government does not block them. The Governments in some countries, such as Saudi Arabia and Iran, block such websites but in Palestine, it is not the Government which blocks them, but parents who mainly do that through the internet providers in the interests of their children.

So the production, dissemination, display or possession of pornographic materials and records are criminalized in Palestine. Whoever is harmed, (it is not only for the protection of children, as is the case in many countries in the world), including adults are all protected.

Article (319) of the JCC criminalizes selling or gaining for the purpose of sale or distribution any obscene material printed or manuscript or photograph or drawing or sample or anything else which leads to the corruption of public morals, or printing or reprinting such objects or materials in any other manner for the purpose of sale or distribution. It also criminalizes the management or the participation in the management of a shop dealing with the sale or dissemination or display of profanity in print or manuscript or photograph or

146 The commentary of article 118 of the MCC.

147 The issue of possession of child pornography is dealt with in Article 3(1)(c) of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

148 Article 118 of the MCC.

149 International Telecommunication Union (ITU).

150 See articles 319 and 320 of the JCC.

drawings or models or any other things that might lead to the corruption of public morals. Broadcasting, by any means, is also criminalized. At the same time, article (320) of the same law criminalizes any abusive conduct or obscene gesture which is considered as contrary to decency, or showing any signal contrary to modesty in a public place, or in a private place where anybody located in a public place can see it.

From the foregoing analyses, we can conclude as follows:

1 Producing, selling, publishing, dissemination, or displaying pornographic materials are prohibited acts;
2 The prohibited materials include tangible materials such as magazines and hardcopy materials, which are considered as offensive and lead to the corruption of public morals. This means that intangible products and materials (such as soft copy materials) are not criminalized in line with the doctrine that criminal law must be construed narrowly.
3 The act should be intentional and aimed at conveying the offensive materials to the public.
4 Producing or displaying any offensive material for one's own enjoyment is not a crime. Therefore, photographing oneself naked or producing a video of sexual practice with one's wife for their own use is not prohibited.
5 Pornography includes both the real and the virtual one in which animated puppets are used.
6 Child pornography is criminalized, since it is included in pornography as a whole, without any difference in the elements of the crime or the severity of the punishment.
7 The possession of child pornography, either tangible or intangible, as long as it's for one's own use, is not criminalized under the JCC.

5.3.2 Religious, Press and Hate Speech Offences

Religious offences are offences motivated by religion such as insults related to religious symbols. A press offence can be defined as "an offence which has been committed by means of the press and which has been given a certain actual publicity and is an expression of opinion".[151] The International Covenant on Civil and Political Rights covered the basic rights which everyone shall enjoy, including the right to freedom of thought, conscience and religion (article 18). It assured that everyone shall have the right to freedom of expression (article 19). Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law (Article 20).

151 Paul De Hert, supra note 75 at 906.

Unlike the CoE Convention on Cybercrime, which did not tackle religious, press and hate speech offences expressly, the Arab Convention on CITO covered offences related to terrorism, committed by means of information technology, including spreading religious fanaticism and dissention and attacking religions and beliefs (article 15).

At the national level, the legal systems differ extensively between societies worldwide. In Palestine, there exist provisions criminalising the insult of religions.[152] Concerning the press and hate crimes, the law provides that the press functions freely in providing news, information and comments and contribute to the dissemination of thought, culture and science within the framework of law and the preservation of freedoms and public rights and duties and respect for the freedom of private life and inviolability of others.[153] Meanwhile, the press shall refrain from printing what is contrary to the principles of freedom, responsibility, human rights and respect for truth and freedom of thought, opinion and expression. Otherwise, press crimes may be committed. Furthermore, periodicals of children and teenagers must not contain any pictures, stories or news which violate morals, values and traditions of Palestinians.[154] The law also states that every journalist must respect the ethics of the profession, including refraining from publishing anything that fuels violence, intolerance and hatred or calls for racism and sectarianism.[155]

In general, the press is prohibited from publishing the following: essays and articles that contain contempt of religions and doctrines, and articles that would offend the national unity or incite people to commit crimes or create hatred and provoke sectarianism among community members.[156] The press and printing shall be guaranteed and the freedom of opinion is guaranteed for every Palestinian, who may express his/her opinion freely in words, writing,

152 Article 273 of the JCC states that "Anyone publicly disrespects divine prophet is imprisoned from one year to three years", whereas article 278 of the same law states that "shall be punished with imprisonment not exceeding three months or a fine not exceeding 20 JD each anyone who:

1. publishes a script, a picture, a graphic or a symbol that would lead to insulting religious feelings to other people or to insult religious beliefs; or
2. utters in a public place and the glare of another person with a word or a voice, which might insult the religious belief of that person".

153 Article 3 of the Law of Press and Publication, published in volume no. 6 of the Palestinian Official Gazette on August 29th, 1995.

154 Article 7 of the Law of Press and Publication.

155 Article 8 of the Law of Press and Publication.

156 Article 37 of the Law of Press and Publication, published in volume no. 6 of the Palestinian Official Gazette on August 29th, 1995.

illustration in any means of media.[157] To answer the traditional question whether the conventional provisions of law on "religious and press crimes" are applicable to actions committed over the internet, one can say that such provisions are accepted as being applicable to crimes committed through the internet. For example, the Palestinian courts have rendered some judgments which criminalised bloggers who insulted the president of the PA and the other Palestinian officials and institutions over the internet.[158] This is similar to Belgian courts' judgments. In 2004 defamation on a website was qualified as a press crime by the Court of First Instance of Brussels. The same court in 2009 equally found a press crime in the act of posting defamatory comments below an online video.[159] The court ruled that "the process of multiplying a blogged article through a website is comparable to the process of reproducing it through classic paper printing".[160] Finally, one should bear in mind that the legal approaches to criminalizing illegal content should not interfere with the right to freedom of expression, but they may subject it to restrictions.[161]

5.4 *Offences Related to Infringements of Copyright and Related Rights*

The main international instruments on copyright and related rights are the Berne Convention for the Protection of Literary and Artistic Works (Paris text 1971), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the WIPO Copyright Treaty.[162] The Convention on Cybercrime urges the State Parties to the convention to adopt legislative and other measures as necessary to establish criminal offences under their domestic law regarding the infringement of related rights pursuant to the obligations they have undertaken under the abovementioned instruments.[163] The Berne Convention for the Protection of Literary and Artistic Works (Paris text 1971) aims to "protect the rights of authors in their literary and artistic works". "The expression "literary and artistic works" shall include every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, such as books, pamphlets and other writings; lectures, addresses, sermons and other

157 Article 2 of the Law of Press and Publication.

158 For example, the Bethlehem Magistrate Court rendered a judgment in 2013 convicting a blogger who insulted the PA President via his website on the Facebook. The penalty was imprisonment of one year. Fortunately, the President used his constitutional right of amnesty, so the penalty was not inflicted.

159 Paul De Hert, supra note 75 at 907.

160 Court of Appeal of Mons, May 14th, 2008.

161 Gercke, Marco, supra note 49.

162 Adopted in Geneva on December 20, 1996.

163 Article 10 of the CoE Convention on Cybercrime.

works of the same nature; dramatic or dramatic-musical works; choreographic works; musical compositions with or without words; cinematographic works to which are assimilated works expressed by a process analogous to cinematography; works of drawing, painting, architecture, sculpture, engraving and lithography; photographic works to which are assimilated works expressed by a process analogous to photography; works of applied art; illustrations, maps, plans, sketches and three-dimensional works relative to geography, topography, architecture or science".

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) in its preamble desires to reduce distortions and impediments to international trade, taking into account the need to promote effective and adequate protection of intellectual property rights, and to ensure that measures and procedures to enforce intellectual property rights do not themselves become barriers to legitimate trade. Article 10 of the convention states that computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971). The WIPO Copyright Treaty considers that copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts. According to the treaty, computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression.[164] The Arab Convention on CITO also covered offenses related to copyright and related rights. It criminalized the violation of copyright, but relies on the law of the State Party to define and enforce the convention provisions. In the case of Palestine, the law which regulates copyright is the Copyright Law of 1911.[165] The rights protected by this law are all the literary, dramatic, musical and artistic rights. The law defines copyright as "the right which a person has to issue or to re-issue any idea physically, or any substantial part of it, and the right to represent and play in drama any story or novel, or any substantial part of it, in public".[166] The law protects the copyright of an author as long as he/she is alive and 50 years after his/her death.[167]

164 Article 4 of the WIPO Copyright Treaty, available at the website: http://www.wipo.int/treaties/en/ip/wct/ (cited on July 28th, 2015).

165 This law dated back to the Ottoman Empire period in its rule over historic Palestine among other Arab Countries which used to be governorates under the rule of the Turkish state from Istanbul (1516–1914).

166 Article 1 of the Copyright law of 1911, published in a special volume of the British Mandate to Palestine Official Gazette on January 22nd, 1937.

167 Article 3 of the Copyright law of 1911.

The abovementioned international instruments which Palestine is eager to ratify and accede to, were drafted in the very early age of the internet, and do not take newer developments sufficiently into account. Since then many important technological developments have taken place, such as file-sharing systems, which enable unconstrained swapping of music and video files.[168] Of course, the domestic copyright law, which dates back to 1911, is much older and was enacted before the invention of the computer and the internet. Therefore, the Palestinian legislature is invited to amend the law, or to enact a new copyright law, to be consistent and adaptable to the new technological developments.

6 Concluding Remarks

At the end of this research paper, the following points and conclusions are apparent:

- It is evident that the JCC is ill equipped to deal with and to criminalize cybercrimes effectively.
- Legal reform is crucial, but not sufficient. Technical approaches, public awareness and ethical online education are vital as well.
- It is difficult for the Palestinian authorities to execute the drafting process for cybercrime law without international cooperation, due to the rapid development of network technologies and their complex structures.
- It is also necessary to monitor the development of international standards and strategies. Consequently, international attempts to harmonise different national penal laws are increasingly important.
- Cybercrime knows no borders and it is just one click away. Therefore fighting it needs the cooperation of the international community, as a whole, including the different formal and informal agencies in each country such as telecommunication institutions, service providers, companies involved in internet security, financial institutions, experts, and relevant civil society organisations.
- The Palestinian legislature should enact a cybercrime law, which is compatible with the CoE Convention on Cybercrime, or incorporate the Arab Convention on CITO in to the Palestinian legal system.

168 Polanski, Paul Przemyslaw, the internationalization of internet law, in: J. Klabbers, M. Sellers (eds.), The Internationalization of Law and Legal Education, Ius Gentium: Comparative Perspectives on Law and Justice 2, Springer Science+Business Media B.V. 2008, P. 207.

- There are two approaches before the Palestinian legislature and decision makers: either to enact new legislation (Criminal Code, Cybercrime Law, Electronic Transaction Law, Telecommunication Law, etc.) including provisions on Cybercrime; or to amend the existing ones to incorporate provisions on cybercrime.
- According to the conventional provisions of law, the punishments meted out by the courts in Palestine are simply light and not proportional to the damage that result from cybercrime. Therefore, aggravated punishments should be inflicted, or an effective alternative to criminal sanctions which lie in civil remedies, might be sought.
- Other methods, including social sanctions, altering the social environment, and education need to be deployed in conjunction with legal sanctions. A logical starting point would be for the media to stop elevating convicted cybercriminals to "pop star" status. Education and courses in ethics are very important.
- Even enacting "modern legislation" such as criminal law, telecommunication law, electronic transaction law and computer crime law is not sufficient. There must be greater efforts at catching up with legislative adjustments in good time. The delay between the recognition of potential abuses of new technologies and amending the relevant laws creates room for abuse.
- In its endeavour to enact relevant legislation to counter cybercrime, the Palestinian legislature should maintain a balance between the interests of law enforcement and respect for fundamental human rights, including the right of everyone to hold opinions without interference, as well as the right to freedom of expression and the right to the protection of personal data. This issue is a problematic and sensitive one, especially in developing countries.