Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.22, 2014

Jurisdiction in Cybercrimes: A Comparative Study

DR. ADEL AZZAM SAQF AL HAIT

Abstract
Cybercrimes were, not long ago, introduced. Such crimes aim at either compromising the vast technical significance of data or misusing such data to commit crimes, not similar to conventional crimes, except that they are committed in the cyber- world. Consequently, modern societies face major losses and risks. Cybercrimes are committed in the shadows, transmitted worldwide by-passing boarders and check points, without the need for documents or personal information. Moreover, they are usually committed by smart, technically knowledgeable, evidence erasing capable criminals, who change locations to hit once again. All these factors make committing such crimes easier.Countries of the world face serious challenges related to enforcing their penal laws upon cybercrimes committed in other countries whose criminal result extends to their territories; the problem arises in respect of subjecting the cybercriminal to trial if he/she commits the crime in a country while its result occurs in another country and the victim may has nationality of different country, then, which country is more entitled to prosecute the convict? To what extent does the matter relate to the bilateral extradition treaties and international conventions? This study aims to discuss and analyze problem of jurisdiction over the cybercrime, extradition law of cybercriminals, international conventions, and related judicial laws and applications especially in the American, British, and Jordanian jurisprudence, along with the related United Nations conventions.
This study concluded that any cybercrime is undoubtedly a translation of the criminal ideas into digital language, thus the criminal responsibility exists when crime terms achieved, no matter whether by traditional or electronic means. It also concluded that cybercrime laws must be harmonious among different countries; since they protect the common interest.
Keywords: Cybercrimes, Jurisdiction, cyber-world

1. Introduction

Cybercrime is a concept that has different definitions. The United Nations has not provided for a universally accepted definition of cybercrime. Literally, cybercrime pertains to a crime related to the cyberspace, computers, networks and the internet. In general, cybercrimes may be categorized under the following areas: (a) computers and networks as tools for criminal activity which includes spamming, email bombing and defamation, hate speech and violation of copyright laws; (b) computers and networks as targets of criminal activity such as unauthorized access, data theft, computer hacking, denial of service, and attacks using malicious code; c) computers and networks as place of criminal activity such as financial fraud; d) computers and networks as new facilitators for older crimes such as online child pornography, online gambling, phishing, espionage and terrorism (Subramanian & Sedita, 2006, p. 40).
In the cyber-world, there are no definite territories or boundaries. The entire world is just a simple click away. This makes the prosecution of cybercrime exponentially difficult for local law enforcement. While domestic police, prosecutors and courts can only operate within their particular territorial jurisdiction, criminal activity and behavior recognizes no borders. It is therefore imperative for states to develop legal tools to deal with cases where one or more of the location of the crime, the accused, evidence, or criminal proceeds is in another country (Laura Barnett, 2008, p. 1).
The importance of having legal tools that can effectively deal with cybercrime is highlighted in the case of 'Love Bug' virus. (Brenner & Koops, 2004, p.6) In 2000, the Love Bug virus spread throughout the world causing billions of dollars in damages in different countries. The source of the 'Love Bug' virus was eventually traced in the Philippines. With the help of the Federal Bureau of Investigation, the Philippines' National Bureau of Investigation identified a certain Onel de Guzman as the person who created the virus and uploaded it in the worldwide web. While there was sufficient evidence against Onel de Guzman, the government prosecutors faced a serious obstacle before they could file charges against him. It was found out that at the time of the commission of the crime, the Philippines had no law against computer hacking (Brenner & Koops, 2004, p. 7).
According to the Department of Justice who reviewed the charges against Onel de Guzman, the provisions of Access Devices Regulations (RA 8484) is inapplicable in his case since the said law only applies to the fraudulent use of credit cards to obtain credit for services of goods. Article 308 of the Revised Penal is also inapplicable since the suspect's criminal intent to gain which is an element in crime of theft was not established. Thus, following the legal principle of "There is no crime when there is no law punishing it" the charge against Onel de Guzman was dismissed (Brenner & Koops, 2004, p. 7).
While it is essential for the nations to have their own legal tools against cybercrime, it is more essential for these laws against cybercrimes to be harmonized. The need to harmonize laws against cybercrime is highlighted in the recent case against Yahoo. Yahoo has a website which auctions in France Nazi Memorabilia and Third Reich

related goods. French law, however, prohibits the display in France of Nazi souvenirs for the purpose of sale. Moreover, the online sale of Nazi artifacts in France is considered as an offense on the memory of France which was severely wounded by the atrocities committed by the Nazis during World War II (Carl S. Kaplan, 2000, p.2). On the other hand, Yahoo argued that it is a company incorporated in the United States of America and the laws of France is not binding upon it. The French High Court ordered Yahoo to prohibit internet users in France from gaining access to the auction of Nazi-related objects. It was also ordered to remove these auctioned items in its server for being in violation of its laws ("Yahoo! loses Nazi auction case", 2000).

The Yahoo case illustrates the possible complications that may arise when the laws of one country against cybercrime conflicts with the laws of another country. As noted above, in the French laws prohibit posting of the Nazi Memorabilia but the laws of USA do not prohibit such acts (Carl S. Kaplan, 2000). This also presents a thorny issue for a nation which wants to prosecute a cybercrime committed by perpetrator within the territory of another nation. What if the damage caused by the act of a cyber criminal reaches the territory behind borders? What if the committed act was not a crime in the country of action but considered a crime in the country that damage reaches its territory? If both countries want to file charges against the perpetrator which country shall be given priority? Which country has jurisdiction to file charges against the perpetrator of the crime? What if no state wants to file charges against the perpetrator of the crime? What should be the basis for claiming jurisdiction over the criminal act? Should it be the territory where the crime was committed or the nationality of the person committing the act or the country of residence of the perpetrator?

In answering these questions, it is important first to define the concept of jurisdiction. Jurisdiction is the sovereign authority of a nation to make laws which are enforceable within its own territory (Brenner & Koops, 2004, p.5).

The international judicial jurisdiction and the public judicial jurisdiction of Hashemite Kingdom of Jordan courts are intended to draw the limits where the state exercises its judicial powers corresponding to these limits, and where other countries are exercising their judicial authorities.In fact, judicial jurisdiction dispute is differs from conflict of laws in that the latter represents binary rules, or at least, it might be binary, in the sense that the national legislature, during its formulation, undertakes presenting the National Law authorities and the cases that allow implementing the foreign law in their territory; while on the contrary, we find that judicial jurisdiction rules is single sided, meaning that the national legislature draws the limits of the national courts' jurisdiction, but does not distinct the limits of foreign courts' jurisdiction, due to that the rules of judicial jurisdiction in addition to the courts exercising the right of judiciary is a manifestation of sovereignty, and one important function of the State as well; Accordingly the national character is more prominent in organizing judicial jurisdiction's dispute, than in the legislative jurisdiction (cassation, Amman, No. 2825/1999).

2. Jurisdiction over Cybercrimes and the International Conventions

2.1 UNTOC and Jurisdiction over Cybercrimes

On November 15, 2000, the General Assembly adopted the United Nations Convention on Transnational Organized Crime (UNTOC). Presently, it is the United Nations' main international treaty that deals with transnational organized crime. It is a manifestation of the United Nations' commitment to fight transnational organized crime.

While there is nothing in UNTOC which define cybercrime within its provisions, cybercrime can be covered under its articles, when cyberspace is used as an environment for committing organized crimes. On one hand, cybercrime is inextricably linked with organized criminal group. There is evidence that sophisticated criminal groups have taken advantage of internet technology for purpose of committing different crimes such as online pornography, hacking, money laundering, fraud and theft.

On the other hand, cybercrime is transnational in nature. Section 3 of the UNTOC states that an offense is transnational in nature if:

(a) It is committed in more than one State; *(b)* It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State; *(c)* It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or *(d)* It is committed in one State but has substantial effects in another State (Section 3, United Nations Convention on Transnational Organized Crime).

In the cyber-world, computer crimes can be committed by a perpetrator who is located in one country against a victim who may also be located on a different country. This crime may also be committed in several countries at the same time. In the same manner, persons responsible for committing cybercrime can easily transfer location from one country to another in order to elude detection and arrest.

In view of the transnational nature of cybercrime and its association with organized criminal group, the UNTOC can be used as basis for adopting measures to gain jurisdiction on various computer-related crimes. Article 15 of the UNTOC establishes the criteria by which the contracting parties to the convention may acquire jurisdiction over the offenses covered by UNTOC.

It states that the contracting parties to the convention may establish jurisdiction on crimes covered by the convention when the offense is committed within its territory. This is a restatement of the Territorial principle of the criminal law which states that all crimes committed within the territory of a country shall fall under its jurisdiction. Jurisdiction over computer-related crimes may also be established when the offense is committed on board a vessel or inside an aircraft that is registered under the laws of the country. This is so since vessels and aircrafts are considered as extensions of the territory of a country.

Jurisdiction over computer-related crime may also be established when the victim or the perpetrator of the crime is a national of one of the contracting party to the UNTOC. This is in accordance with the active personality principle. Thus, even if the location of the crime is in a different county when the victim happens to be citizen of another country the latter country may still acquire jurisdiction over the cybercrime. The Jurisdiction may also be acquired by a contracting party to the UNTOC when a cybercrime is committed by a stateless person who habitually resides in the territory of the one of the signatories to the UNTOC. This is in accordance with the passive personality principle.

Jurisdiction over cybercrime may also be acquired by a contracting party even when the crime is committed outside its territory if it is the intention of perpetrators of the crime to commit a serious crime within its territory, under Article 5 part 1. Thus, under the UNTOC, a contracting party acquires jurisdiction over a person who organizes, directs, aids, abets or facilitates the commission of cybercrime involving an organized crime even when it is outside its own territory provided that it can be established that there is an intention to commit the crime within the territory.

Article 15 part 3 in relation to Article 16 paragraph 10 establishes the hierarchy in the claims of jurisdiction when the crime was committed within the territory of a contracting party by a person who is a national of another country. In these cases, when the contracting party whose national committed the crime does not choose to extradite its national in favor of another contracting party, the former is obliged under the convention to prosecute its nationals for the crime committed. In the prosecution of its national for crime committed outside its territory, the convention stated that the perpetrator shall be prosecuted in the same manner as if a crime of a grave nature has been committed. The convention also requires the other states to cooperate with each other in the submission of evidence against the perpetrator.

Article 15 part 4 on the other hand states that if the perpetrator of the crime is present within the territory of one of the contracting parties and the crime was committed against another contracting party, the former which refuses to exercise the option of extradition is obligated to assume jurisdiction over the crime for purpose of prosecution.

Article 15 part 5 adopts to use the method known as a case by case deliberation on the issue of multiple jurisdiction over the same offense committed against different countries. In the event that a cybercrime is committed against several contracting parties, the contracting parties are supposed to coordinate and consult with each other. The objective is to ensure that the actions are coordinated and to ensure success of the prosecution.

2.2 Council of Europe and Jurisdiction over Cybercrimes

The second international agreement that this study will discuss is the Council of Europe Cybercrime Convention. The Cybercrime Convention was signed in 2001 by the United States and 29 other countries in Budapest, Hungary. The multilateral treaty which took effect in July 2004 was the first treaty signed to address the growing problem of cybercrime. The main goal of the Cybercrime Convention is to provide for a common criminal policy by harmonizing national laws with the aim of protecting the society against cybercrime (Henrik W.K. Kaspersen, 2009).

At the first international treaty on crimes committed via the Internet and other computer networks dealing with infringements of copyright, computer-related fraud, child pornography and other violations of network security, it commits signatories to prosecute the violators of computer-related crimes with a firm resolve. It is the goal of the signatories to the treaty to end the cybercriminals' feeling of invincibility by requiring sanctions and making cybercrimes and other computer-related crimes an extraditable offense and by reducing the number of countries that the cybercriminals can avoid prosecution.

The United States was one of the thirty (30) counties that signed the Convention on November 23, 2001 in Budapest. The United States also ratified the Convention on August 3, 2006. As of 2006, there have been forty three (43) countries that signed on the Convention (Henrik W.K. Kaspersen, 2009).

Towards this end, the contracting parties to the treaty are required to define criminal offenses and sanctions under their own domestic laws for the four categories of computer-related crimes such as fraud and forgery, child pornography, copyright infringements and security breaches. The treaty also requires the signatories to establish domestic procedures for detecting, investigating and prosecuting computer crimes and collecting electronic evidence and to establish a rapid and effective system of international cooperation.

Articles from (27-35) defines the procedures related to requests for mutual assistance, in the absence of enforced international agreements; and the necessity to maintain the confidentiality of information's request, the mutual assistance regarding the urgent precautionary procedures on stored computer data related to crime and the speed

in detecting confidential stored data traffic and mutual assistance relating to each of: accessing stored computer data and crossing the limits, and accessing stored data in any geographic location, in a state, which is a party in an agreement; in addition to compiling the data traffic in a fast way and challenging data content. As stipulated in Article (35) to maintain a point of contact available on a twenty - four hour, seven days a week basis, for the purposes of investigations or proceedings concerning criminal offences related to cybercrimes to any of States Parties, or to collect evidence, or to provide technical advice, or to preserve the data.

In fact, the articles that regulate the jurisdiction of States Parties were stipulated in Article (22) of section 3 of the Convention related to Cybercrime (Budapest, 2001, Group of the European Treaties, the Europe Council, No. 185). This article, in its first paragraph, stipulates the possibility that the Contracting Parties impose their jurisdiction over any offence established in its territory, covered by this convention. This text is considered a repetition to the principle of regional criminal law that states, that all crimes committed within the territory of a state, falls under its jurisdiction. And the judicial jurisdiction might be determined on the crimes of the virtual world as well, when a crime is committed on a ship board or on board an aircraft registered under the laws of the concerned country, where the ships and aircrafts are considered as an extension of the territory of that state. In other cases where the state party in the convention of an individual that committed a crime, choose not to extradite one of its citizens for the benefit of another contracting party, as stated in the third paragraph of Article (22). The first contracting party is obliged, under the present convention, to prosecute its citizen that committed the crime. And in case this state prosecute its citizens for the committed crime that its criminal activity extended outside its territory, the convention obliges to prosecute the criminal in a manner as if such crime that is committed outside its territory had been committed within its territory, and on the same degree of risk. The convention also stipulates that states parties shall cooperate with each other in collecting evidence against the criminal Also, the Article (24), title 2, organized the mechanism of cyber criminals extradition, where the third paragraph states that this convention is considered extradition convention in case the related states parties were not signatory in other convention that address the same subject; as stated in the fifth paragraph: “The convention respects the principles of national extradition in the States Parties, including the grounds on which the requested Party may refuse extradition”**.**

While the fifth paragraph of Article (22) adopts the principle of using the method known by the term: "Discussing each case separately," regarding the issue of multi-jurisdiction for the same crime committed against different countries. In case the committed crime was against a number of contracting parties, these parties are obliged to coordinate and consult each other in order to ensure that efforts procedures are coordinated to ensure the success of the trial.

In fact, Group of Eight - G8 (France, Germany, Italy, Japan, United Kingdom, United States, Canada and Russia) have decided, as we have mentioned earlier, to have a permanent control point for the Internet, operates around the clock, to give a warning as soon as one of hackers penetrate the International Network; Once the alarm starts, some of the finest specialists in the Cyber crime world, work to locate the suspect, tracing his e-mail and to identify his criminal activity’s area. Among the objectives that the European Council is trying to achieve is setting a remote inspection system, so the informational police officer can inspect the suspect’s computer, remotely; and to expand the concept of internet crime, so to criminalize any person access any confidential network’s information that is not dedicated to the public, without a license.

3. Jurisdiction over Cybercrimes and the National Laws

3.1 United States Laws Jurisdiction over Cybercrimes

Before prosecution against any individual or organized criminal group may proceed, the USA court must have jurisdiction over the crime involved. As a rule, the court has declared that there is a presumption that the laws of the United States do not have extraterritorial application (United States v. Cotton, 471 F.2d 744). This is due to the necessity of avoiding conflicts with foreign laws which may result from the enactment of laws with extraterritorial application.

In the past few decades, however, Congress has passed laws that can support the exercise of criminal jurisdiction even beyond its territory. Indeed, it is beyond question that Congress has the authority to enforce its laws beyond the territorial boundaries of the United States. For instance, Section 1029 of the USA Patriot Act of 2001 was purposely revised by Congress with the intention of providing extraterritorial jurisdiction for the acts covered by this section. Section 1029 (h) provides that:

Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if:

(1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and

(2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of

such offense or property derived therefrom (18 U.S.C. § 1029 / h).

State laws have also been passed providing for extraterritorial application of the state's criminal laws. These statutes enable one state to assert jurisdiction for violation of its own laws even when the crime is committed outside of the territory of the state. In North Carolina, for instance, cyberstalking is committed even when the person who sent electronic mail or communication is outside North Carolina:

"Any offense under this section committed by the use of electronic mail or electronic communication may be deemed to have been committed where the electronic mail or electronic communication was originally sent, originally received in this State, or first viewed by any person in this State" [N.C. Gen. Stat. [section] 14-453.2 (2002)].

A similar law can be found in Arkansas which grants it jurisdiction to prosecute computer crimes committed outside of its jurisdiction. It states that:

"a person is subject to prosecution in this state for any conduct proscribed by this subchapter, if the transmission that constitutes the offense either originates in this state or is received in this state" Ark. Code Ann. [section] 5-27-606 (2003).

The recent case of Olez Zezev highlights the extraterritorial application of domestic laws of the United States. It appears that in March 2000 Zezev manipulated Bloomberg's software to bypass Bloomberg's security system for the purpose of gaining unauthorized access to Bloomberg's computer system. Zezev then illegally entered Bloomberg's computer system and accessed different accounts including the accounts of Michael Bloomberg and his employees. He also copied internal information from Bloomberg that can be accessed only by Bloomberg's employees. Subsequently, Zezev sent Bloomberg an email message from Kazakhstan under the alias Alex where he attached various screens which prove his ability to access the account of Bloomberg. He then threatened Bloomberg saying that unless Bloomberg sends him $200,000 he will disclose to the media and Bloomberg's customers what he had done so as to destroy his reputation (Charleston D., 2003).

In response, Bloomberg sought the help of FBI agents which instructed him to send emails to Zezev saying that if he wanted money he would have to meet with Michael Bloomberg in United Kingdom and explain to them how he was able to break into Bloomberg's system. When they met in United Kingdom, Zezev was arrested. He was subsequently indicted. In this case, the email was sent by Zezev from his home country in Kazakhstan. Yet the United States exercised its jurisdiction over the case.

3.1.1 Case of US v. Gorshkov, 2001 Wl 1024026

In 2000, the FBI found out that there has been a series of breaking into the computer systems of various businesses in the United States. The FBI identified the persons responsible as Vasiliy Gorshkov and Alexey Ivanov who are both Russians. The FBI devised a plan to lure them into the United States by creating a corporation called Invita. Gorshkov and Ivanov were then invited to the company for an interview. During the interview Gorshkov and Ivanov were asked to demonstrate their skills in computer hacking. They were provided by the FBI a laptop computer to access their home computers where they keep their hacking tools. The Russians did not know that the FBI used a tool to get the user id and password of the hackers. The Russians were immediately arrested after the demonstration. Subsequently the FBI without a search warrant used the user id and password captured from the laptop to download the information from Gorshkov and Ivanov's home computers in Russia which they used as evidence against the parties. After they were charged for the computer crime, Gorshkov moved for the suppression of the evidence obtained from the home computers which violate the Fourth Amendment and the Russian Law (US v. Gorshkov, 2001 Wl 1024026).

The main issue in this case is whether the defendants' right against unreasonable searches and seizures under the Fourth Amendment were violated when the FBI downloaded from their home computers in Russia. On one hand, the researcher may argue that Russia is a sovereign country, and thus the United States as a matter of comity should have sought permission from Russian authorities to search the computer of Gorshkov and Ivanov. On the other hand, the FBI argued that since the act of downloading from a computer source does not constitute a search it is not necessary for the FBI to secure consent from Russian authorities.

The court denied the motion of the Russians. The court denied the motion of the Russians, relied on the fact that the Fourth Amendment may be invoked only when there is search and seizure within the meaning contemplated by the Fourth Amendment. However, the act of downloading information form a computer in another country by the FBI agents do not constitute a search or seizure since the copying of the data on the Russian computers did not interfere with the possessory interest of the defendant in the data. In this case, the data remained intact, unaltered and accessible to the defendant. Moreover, it would not have been possible for the FBI agents to first secure a warrant of arrest before they can download the data as it would have been possible that the defendant's co-conspirators could destroy that evidence (US v. Gorshkov, 2001 Wl 1024026).

3.2 United Kingdom Laws Jurisdiction over Cybercrimes

The Computer Misuse Act 1990 is the relevant law that establishes jurisdiction on the United Kingdom for violation of cybercrime. The crimes covered by the law are various acts of computer misuse which are defined under Sections 1 to 3 which include unauthorized access to computer material, unauthorized access with intent to

commit or facilitate commission of further offense and unauthorized modification of computer material.
The United Kingdom adheres to the principle of territoriality. However, in the event that the offense takes place outside of the United Kingdom, it shall still have jurisdiction to try the perpetrator of the crime under the Computer Misuse Act of 1990. The relevant provisions are Section 4 and 5 which states that it is not necessary for the cybercrime to be committed within the territory of United Kingdom so long as the offense is significantly linked to the United Kingdom. Thus, even the act committed is not a crime in the place of commission but it is a crime in United Kingdom and it is established that the offense is significantly linked to it; the Computer Misuse Act of 1990 may be applied for purpose of prosecution.
Since the United Kingdom is a member of the European Union, the deficiency in the cybercrime laws of United Kingdom may be supplemented by the Council of Europe Cybercrime Convention. Article 22 of section 3 in the Convention provides for the rules when the contracting parties to the treaty are obliged to establish jurisdiction over the criminal offense. Paragraph (a) is a restatement of the principle of territoriality which is a basic characteristic of criminal law. It states that the contracting parties shall adopt legislations necessary to punish the commission of crimes defined in the treaty that are committed within its territory.
Paragraph (b) and (c) are also based on the principle of territoriality. When the crime is committed on board a ship or an aircraft registered under the laws of the United Kingdom while passing through the territory of United States, is the United Kingdom deprived of its jurisdiction to prosecute the offense? Following paragraph (b) and (c) the treaty requires that contracting parties to establish jurisdiction over criminal offense committed inside its ship or aircraft registered under its name. As a matter of legal principle the crimes committed inside the ship or aircrafts of a particular nation even when they are outside its territory are still considered committed within its territory since they are considered as extensions of the territory of the state.
Paragraph (d) on the other hand is a restatement of the principle of nationality as basis for conferring jurisdiction upon a state. It states that the nationals of a particular state are not immune from criminal liability of their own state even if they are outside its territory. They are still obliged to comply with their domestic law even when they are beyond the territory of their own state. For instance, a British man who goes to a country which does not have a law against hacking and while within the territory of the country uses a computer to hack through a computer of a person in the United Kingdom is still within the jurisdiction of his own state.
In 2003, a new extradition treaty between the United Kingdom and Northern Ireland and the United States of America was signed. The new extradition treaty which is a supplementary to the extradition treaty signed at London in 1972 and amended by Supplementary Treaty signed at Washington on June 25, 1985, is a reflection of the modern practice in extradition.
It states that any crime that is punishable by a maximum sentence of or more in both the requesting and the requested state is extraditable. In Article 2, the new treaty states that: “An offense shall be an extraditable offense if the conduct on which the offense is based is punishable under the laws in both States by deprivation of liberty for a period of one year or more or by a more severe penalty”.
It is worth nothing that the new treaty avoided making an enumeration of extraditable offense which was done in the 1972 treaty. With the use of dual criminality clause in Article 2, there is no longer any need to amend or supplement the new treaty as new offenses become punishable under the laws of both states. The new treaty therefore looks forward into the future by including any other offenses that may be punishable under the laws of both states by imprisonment of one year or more.
Moreover, the new treaty encompasses offenses which are previously not punishable under the 1972 treaty. Thus, new treaty also looks backward by covering all offenses although not previously mentioned in the 1972 treaty.

3.2.1 Case of Gary McKinnon Case

In 2001 and 2002, Gary McKinnon, a systems administrator in United Kingdom, hacked into 97 United States military and NASA computers from his home computer. After he hacked the computers, he deleted data from these computers which included the following: a) critical operating system files which result in the shutdown of the entire United States Army’s Military District of Washington Network of over 2000 computers for 24 hours; b) 2,455 user accounts on a US Army computer and their control access to an army computer network which caused the computers to reboot and become inoperable; c) the logs from computers at US Naval Weapons Station Earle which was being used for monitoring the identity, location, physical condition, staffing and battle readiness of Navy ships. With the deletion of these files, the United States for several hours became vulnerable to intruders. Moreover, the defendant also copied data and files into his own computers which include operating system files containing account names and passwords from 22 computers among them are files from US army computers, 35 files from US Navy computers, and 6 from NASA computers. Investigation by the UK National Hi-Tech Crime Unit revealed that Gary McKinnon was responsible for the intrusions and he was arrested under the Computer Misuse Act. No charges were brought by UK against McKinnon. Later, a new Extradition Treaty was signed between the United States and the United Kingdom. Because the crime was covered under the Extradition Treaty between the United States and the United Kingdom, the United States advise the United

Kingdom that it will be requesting for the extradition of Gary McKinnon. Charges were filed against Garry McKinnon in August and September 2004 in Districts of Virginia and New Jersey which subsequently issued a warrant of arrest against him.

Gary McKinnon's legal team challenged his extradition on the ground that the location of the criminal act, the facilities and the computers were all in the United Kingdom. For his legal team, it was their strategy to invoke United Kingdom's jurisdiction over the case. Reason is simple; the United Kingdom has a long history of being lenient to those who commit computer crime (Tom Espiner, 2009). Under UK's Computer Misuse Act, the maximum penalty is only five years. On the other hand, if ever McKinnon will be extradited he may face up to 70 years if found guilty of hacking computer military system ("CPS Decision on Gary McKinnon Case", 2009, p.1).

In May 2006, however, the judge at Bow Street Magistrates' Court has ruled that McKinnon should be extradited. In addition, Home Secretary John Reid has signed an order allowing McKinnon's extradition to the United States. Moreover, the Crown Prosecution Service (CPS) has announced in February 2009 that it will not exercise its jurisdiction over the case. Alison Saunder, the head of the CPS Organized Crime Division has said that while the act may have been committed using McKinnon's home computer, "the target and the damage were transatlantic." Moreover, CPS found that there is insufficient evidence to prosecute McKinnon under Section 3 of the Computer Misuse Act since it was not established whether there was malicious intent on the part of McKinnon. The decision of the Crown Prosecution Service not to prosecute McKinnon rests on the provision of the Computer Misuse Act of 1990 which grants United Kingdom jurisdiction over an offence only when the offense is significantly linked to the United Kingdom ("CPS Decision on Gary McKinnon Case", 2009, p. 1).

3.3 Jurisdiction for Cybercrimes in the Jordanian Law

The issue of jurisdiction in the virtual world is considered one of the relatively recent problems, particularly in Jordan, where the traditional provisions in the Criminal Procedure Code, as amended, No. 9, 1961, and the Penal Code No. 16 of 1960 - set out, in general, the rules of jurisdiction in criminal cases; thus, there is not any provisions, in particular, extend the jurisdiction of Jordan courts on cybercrime, but it is included legally in the provisions applicable to penal crimes, with the exception of the fourth paragraph of Article (5) in the Code of Criminal Procedure; and it has been stated in the text of this article as follows:

Article (5):

1. The common right lawsuit shall be instituted against the defendant before the competent judicial authority to which the place of committing the crime, the domicile of the defendant or the place of arresting him is located within his area of jurisdiction. No preference for a reference over another except by the prior history of the prosecution.

2. In case of attempt, the crime shall be considered as committed in each place where any act of attempt takes place. In case of permanent crimes, each place where the state of continuity occurs shall be considered as the place of committing the crime. In regard of habitual and sequential crimes, the crime place is each place any of the crime acts is involved.

3. If a crime was committed abroad and was one of those on which the provisions of the Jordanian law are applied, and its perpetrator has no known place of residence in the Hashemite Kingdom of Jordan, and was not arrested there, then the common right lawsuit shall be instituted against him before the judicial authorities in the capital.

4. The common right lawsuit shall be instituted against the defendant before the Jordanian judiciary, if the crime was committed by electronic means outside the Kingdom, and its effects resulted there, in whole or in part, or on any of its citizens. "

The general rule in jurisprudence, in various countries around the world, including Jordan is that the jurisdiction of the electronic crimes committed via the Internet takes place where the crime outcomes are; and thus, it is the same if the perpetrator of the criminal activity is a resident in a distant country, or he or she lives near the victim house. Often, what matters is the place of the crime outcome, and this was confirmed by the fourth paragraph in the aforementioned Article (5).

Recently, however, The Council of Ministers in its meeting held on 30.08.2010, sanctioned the final formula of the Interim Information Systems Act number 30 of 2010, where Article (16) of the Act states an emphasis on the same principle stipulated in the aforementioned Article (5), which states:

"Public right and personal right litigation may be filed against the defendant before the Jordanian judiciary if he/she commits any crime stipulated in this Act using information systems inside the Kingdom that harms any of its interests or any of its residents or, in whole or in a part, it has the crime consequences within its territory or committed by one of its residents".

In regard to the jurisdiction of the person, the Jordanian legislator set out in Article (10) of the Jordanian Penal Code the following text:

The provisions of this code shall be applicable on:

1. Every Jordanian whether he was a doer, an inciting accomplice, or an accomplice who has committed a felony

or misdemeanor according to the Jordanian laws outside the Kingdom. The said provisions shall be applicable even if that person has acquired the Jordanian citizenship or has been denaturalized after committing the felony or misdemeanor.

2. The crimes committed outside the Kingdom by any Jordanian official while performing his job or resulted from his practice to that job.

3. The crimes committed outside the Kingdom by the officials of diplomatic corps or the Jordanian consuls who enjoy the immunity granted by the Public International Law.

4. Any foreigner residing in the Hashemite Kingdom of Jordan, whether he was a doer, an inciting accomplice, or an accomplice who has committed a punishable felony or misdemeanor according to the Jordanian laws outside the Kingdom if his extradition was not requested or approved.

This principle is to punish every Jordanian has committed a crime, anywhere in the world, according to the laws of his or her nationality, that are the laws of the state to which he or she belongs; where the national law is defined for each crime committed by those who have the nationality of a state, although committed outside its territory, as (Active Personality Principle), it is the principle adopted by the Arab countries; but Arab countries did not adopt the (Passive Personality Principle) where the national legislation pursues any offender who has committed a crime against a victim who has the nationality of its court, anywhere in the world . This principle assumes that a state where the crime took place inside its territory might exaggerate in protecting its citizens entrusted to its courts the negative jurisdiction (Al Said: 2009, p. 116-117).

Worth mentioning that this application is different, as we have mentioned earlier, from the U.S. and British legislations that adopted principles; the active and passive. Adopting the principle of "passive personality" means the emphasis on extending the punishment authority over each foreign territory, where its citizens are subject to attack, and working accordingly, needs the signing of several bilateral and international extradition agreements.

With regard to the extradition of cyber and normal offenders in the Jordanian jurisprudence, Article (21) of the Constitution of the Hashemite Kingdom of Jordan 1952 stipulates the following:

1. Political refugees are not subject to extradition due to their political beliefs or for defending their freedom.
2. International agreements and laws set the proceedings of extradition for ordinary criminals.

In addition to, the extradition is regulated by Extradition of Fugitive Criminals Act, as amended, for the year 1927 (official newspaper No. 160 dated 01.07.1927), along with a number of extradition treaties signed by Jordan with a number of countries, the most famous are the Riyadh Arab Agreement on Judicial Cooperation of 1983 (official newspaper No. 3329 dated 07/16/1985), and the bilateral judicial cooperation with Arab Republic of Egypt (ratified under the Law No. 3 of 2001, published in the official newspaper No. 3378 dated 03.01.2001), and other agreements.

It is conditioned for extradition, the fulfilling of some substantive and formal requirements, including:

a. The existence of an extradition agreement.
b. The person subject of the extradition is sought to be in the territory of Jordan.
c. Availability of objective conditions specified in the extradition agreement.
d. Availability of formal requirements in the extradition request.

And the objective conditions are exclusive and not to be measured by, for instance, as provided in Article (40) of the Riyadh Arab Agreement on judicial cooperation for the year 1983; which stipulates the following:

"Extradition shall be obligatory with respect to the following persons …..... (c) Individuals convicted in presence or in absentia by the courts of the requesting party requesting in case of a penalty of one year or more severe penalty in respect of acts punishable by the laws of the requested party."

4. Principals of conflicts on Jurisdiction over Cybercrimes

Taking into consideration the relevant provisions of the laws against cybercrime in the United States and United Kingdom, it follows that in a hypothetical case where a British criminal commits a crime of hacking against an American individual in the United States, the jurisdiction over the offense will be as follows:

In the first scenario, considering that computer hacking is punishable as a crime in the United States, following the principle of nationality, the United States may exercise jurisdiction over the crime committed within its territory. In this case, the crime did not take within the United States since the act of computer hacking was done in the United Kingdom. The location of the crime, however, is immaterial since the victim is a national of the United States.

On the other hand, the United Kingdom may not claim jurisdiction over the offense. Following the decision of the Crown Prosecution Service in the Gary McKinnon case, the details of which will be discussed later, it can be argued that while the act of computer hacking was done in the United Kingdom the same does not automatically grant jurisdiction over the crime to the courts of United Kingdom. It should be remembered that Computer Misuse Act of 1990 requires that the offense must be significantly linked within the domestic jurisdiction of the

United Kingdom. In this case, however, the victim was an American who also resides in the United States. The damage also for the crime done took place outside of United Kingdom. Thus, in this case only the United States may claim jurisdiction over the case.

However, if based on the same fact the victim was an American individual who resides in France; it follows that the United States will also have jurisdiction over the offense following the Nationality principle. The United Kingdom may still not claim jurisdiction over the offense since the offense is not significantly linked to it. The jurisdiction of France over the case is questionable since the crime was not directed against it. Moreover, the crime does not affect the national interest of France. For this reason, only the United States can claim jurisdiction over the offense.

5. Conclusion

The cybercrime is an illegal behavior to be punished by the law at which one or more of electronic means used as a tool, environment, or goal to commit the crime". Basically, the cybercrime is a digital activity designed to deal with computer systems through their own language, binary code (0, 1), thus, any cybercrime is undoubtedly a translation of the criminal ideas into digital language.

Every country should have sufficient legislative and judicial capabilities to combat cybercrime and such laws must be harmonious among different countries; since they protect the common interest.

Extradition is considered an exception of rule of Penal Law Regionalism and it is implemented under bilateral or international conventions. Accordingly, if the treaty stipulates that extradition must be carried out in certain crimes, then the provision should be followed since it is binding to the extent contained in the convention between these two countries. If, however, there is no extradition treaty; it, then, should be referred to the internal legislation or international custom of countries required to perform the extradition; which is deemed to be optional in this case. The countries stipulate, in the treaties, that the crime requires extradition must be punishable in the law of the two countries, in application of "Dual Criminality" principle.

It may happen that several countries request to extradite one of the criminals. Then, if a provision found in extradition treaty, it should be followed, and if a provision found in the internal legislation, it should be applied; but, if no solution found in the provisions, then the country required to perform extradition should refer to the precedents it adopted in the past. Some countries prefer to execute extradition to the country on which the crime has been committed, and other countries prefer to extradite the fugitive criminal to his/her own country since he/she is one of its citizens, while some countries give priority to the country asked for extradition in an earlier date. However, we noticed how the major countries impose their rule of laws instead of imposing law of sovereignty. The case of (Olez Zezev) sheds light on the way that United States applies its national law outside borders of its territory.

The researcher, according to facts mentioned in the study, believes that if the result of the cybercrime occurs upon more than one country and in case there is an extradition treaty among the criminal's country and the countries on its territories the crime has been committed, then the criminal should be extradited to country more affected by the crime, and in case the extent of damages is equal, then the priority should be given to the country asked for extradition in an earlier date.

References

Al Sa'ed, Kamel (2009) *An Explanation of the General Rules of the Penal Code, Comparative Study*, Dar El-Thaqafa, Amman, Jordan.

Barnett, Laura, 2008, *International Dimensions of Domestic Criminal Law: Extraterritoriality and Extradition*, accessed November 9 2009, http://www.parl.gc.ca/information/library/PRBpubs/prb0117-e.htm

Brenner, Susan. & Koops, Bert-Jaap 2004, *Approaches to cybercrime jurisdiction* (Report). The Journal of High Technology Law. Suffolk University Law School, accessed November 8, 2009, http://www.highbeam.com/doc/1G1-172599113.html

Broadbridge, Sally, 2009, *The UK/US Extradition Treaty*, accessed November 21, 2009, http://www.parliament.uk/commons/lib/research/briefings/snha-02204.pdf

Charleston Daily Mail (2003) *Hacker gets prison time for threatening N.Y. mayor*, accessed December 4, 2009, http://www.highbeam.com/doc/1P2-9894837.html CNN.com, *Yahoo! loses Nazi auction case 2000*, accessed November 9, 2009, http://edition.cnn.com/2000/TECH/computing/11/20/france.yahoo.02/\

CPS Decision on Gary McKinnon Case 2009, *The Crown Prosecution Service*, accessed November 8, 2009, http://www.cps.gov.uk/news/press_releases/109_09/

Darlington, Roger, 2006, *Crime on the Net*, accessed November 21, 2009, http://www.rogerdarlington.co.uk/crimeonthenet.html

Espiner, Tom 2006, *NASA Hacker Debate Rages On, ZDNet UK*, accessed November 7, 2009, http://news.zdnet.co.uk/security/0,1000000189,39278701,00.htm

High Beam Research, Filipino Reporter, *'Love' bug raps dropped: No crime where there's no law punishing it –*

NBI 2000, accessed November 8, 2009, http://www.highbeam.com/doc/1P1-79225181.html
Kaplan, Carl S (2000), *French Nazi Memorabilia Case Presents Jurisdiction Dilemma*, Cyber Law Journal, accessed November 6, 2009. http://emoglen.law.columbia.edu/CPC/archive/hatespeech/11law.html
Natsui, Takato, 2003, *Cybercrimes in Japan: Recent Cases, Legislations, Problems and Perspectives,* accessed November 20, 2009, http://www.netsafe.org.nz/Doc_Library/netsafepapers_takatonatsui_japan.pdf
TMZnet.com, *Police: Georgia man stalked local Facebook user, captured inside abandoned home 2009*, accessed November 8, 2009, http://www.tmcnet.com/usubmit/2009/04/06/4110964.htm
US Department of Justice 2003, *Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion*, accessed November 7, 2009, http://www.cybercrime.gov/zezevSent.htm
Vander Beken, Tom 2003, *The Third Global Forum on Fighting Corruption and Safeguarding Integrity,* accessed November 10, 2009, http://docs.google.com/gview?a=v&q=cache:AAuGGT_sIw8J:www.ircp.org/uploaded/I-1%2520Tom%2520Vander%2520Beken.pdf+Preventing+conflicts+of+jurisdiction+in+international+corruption+cases+is+very+difficult+since+it+requires+States+to+accept+considerable+limitations+to+their+existing+jurisdictional+claims&hl=tl&gl=ph&sig=AFQjCNHHIPUJDjDuSHn_B4XgbWVlTOGBsQ
Vogel, Joachim 2000, *Towards a Global Convention against Cybercrime*, accessed November 9, 2009,http://docs.google.com/gview?a=v&q=cache:wFHxsqlT5o8J:www.penal.org/pdf/GuadalajaraVogel.pdf+cybercrime+challenge+to+the+global+community&hl=tl&gl=ph&sig=AFQjCNHv5_1-vfglVm6GTwGla_QHn2H9ew
Yong, Pi. *Comparative Research on Convention on Cybercrime and Chinese Relevant Legislations*, accessed November 21, 2009, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/567%20china-d-Comparative%20Research_ed1a.PDF