2-1-2020

Overcoming the conflict of jurisdiction in cybercrime

Abdelmonem Mohamed Magdy Khalifa

The American University in Cairo

School of Global Affairs and Public Policy

OVERCOMING THE CONFLICT OF JURISDICTION IN CYBERCRIME

A Thesis Submitted to the

Department of Law

in partial fulfillment of the requirements for the LLM degree in International and Comparative Law

By

Abdelmonem Khalifa

December 2019

The American University in Cairo
School of Global Affairs and Public Policy

Overcoming The Conflict Of Jurisdiction In Cybercrime

A Thesis Submitted by

Abdelmonem Mohamed Magdy Abdelmonem Khalifa

to the Department of Law

December 2019

in partial fulfillment of the requirements for the LL.M. Degree in International and Comparative Law has been approved by the committee composed of

Professor Hani Sayed

Thesis Supervisor _____
American University in Cairo
Date _____

Professor Thomas Skouteris

Thesis First Reader _____
American University in Cairo
Date _____

Professor Jason Beckett

Thesis Second Reader _____
American University in Cairo
Date _____

Professor Hani Sayed

Law Department Chair _____
Date _____

Ambassador Nabil Fahmy

Dean of GAPP _____
Date _____

DEDICATION

I dedicate this thesis to my father's soul, mother and wife,
who have all been a source of enlightenment and encouragement
throughout my entire life.

The American University in Cairo
School of Global Affairs and Public Policy
Department of Law

OVERCOMING THE CONFLICT OF JURISDICTION IN CYBERCRIME

Abdelmonem Khalifa

Supervised by Professor Hani Sayed

ABSTRACT

This study explores the different approaches to managing the conflict of criminal jurisdiction over cybercrime with the aim of comparing the advantages and disadvantages of each approach. It argues that the most effective solution to this dilemma is to determine certain factors to be considered and evaluated by a body established for such a purpose or by the concerned states themselves in order to decide which country will take the exclusive competence over the cybercrime in accordance with the facts of each individual case and taking into account the characteristics of cybercrime. Establishment of these factors should reflect the interests of the different stakeholders related to cybercrime that include like other crimes the interest of victim(s), criminal(s), and concerned states. As long as it is accepted internationally that the jurisdiction over cybercrime can be established based on territory, active and passive personality, as well as the protective principles, the suggested factors should also include the interests of the state where the crime is committed, the state of the offender's nationality, the state of the victim's nationality, and the state whose vital interests have been affected by the crime. In addition, these factors should contain the interest of criminal proceedings as it is a must to achieve the interests of all the stakeholders. In my opinion, these factors should not be given equal weight as many factors are more relevant than others in light of the cybercrime' particularities and the decision in this regard should be reached on the basis of an aggregate balance of all these factors.

TABLE OF CONTENTS

I. Introduction

The Internet has changed the way individuals, governments, businesses, and other organs of society manage their activities by providing them with many online tools that can facilitate the conducting of such activities. Even though it can improve efficiency, it makes them vulnerable to cybercrime, cyber-attack, and cyber-espionage.[1] In 2011, at least 2.3 billion persons, the equal of more than one third of the total population of the world, had access to the Internet. By the year of 2020, it is anticipated that the number of networked devices will be more than the number of people by six to one which will alter the existing concepts of the Internet. Actually, in the hyper connected world of the future, it will be difficult to see a computer crime or may be any crime, which does not include an electronic evidence associated with Internet Protocol (IP) connectivity.[2]

Indeed, the development and use of virtual banks, electronic money, and online shopping has become one of the main reasons for the development of a new kind of a crime that can be committed far away from the actual crime scene. In fact, the communications in cyberspace may be transmitted through different methods, including local phone companies, Internet service providers, long distance carriers, wireless and satellite networks, and may pass through computers located in different states before attacking targeted systems in many other states. Also, the cybercrime's evidence may be stored on an electronic server in a different jurisdiction far away from where the perpetrator committed the crime.[3]

Nowadays, there is a gradual increase in the numbers, cost, and sophistications of attacks against the infrastructures of information systems by cyber criminals. In reality, such attacks threaten the fundamental and growing reliance upon this technology in

---

[1] David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 Minn. J. Int'l L. 347, 347 (2013).

[2] United Nation Office on Drugs and Crime, Comprehensive Study on Cybercrime, xvii (February 2013), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[3] Ana I. Cerezo ET AL., *International Cooperation to Fight Transnational Cybercrime,* Proceedings - 2nd International Annual Workshop on Digital Forensics and Incident Analysis, WDFIA 2007 13, 14 (2007).

order to manage business, carry messages, and process information by corporations, governments, individuals, and other entities.[4]

Generally, the terms computer crime, information technology crime, cybercrime, and high-tech crime are often used interchangeably for referring to two main categories of crimes. The first one includes those crimes where the computer is the target of the offense such as attacks on network confidentiality and availability as well as the unauthorized access to and illicit tampering with systems, programs or data. Whereas, the second category comprises the traditional crimes like fraud, forgery, and theft which are committed with the assistance of or by means of computers, computer networks and related communications and information technology.[5]

Cybercrimes differ from traditional crimes such as murder, rape, and robbery in several ways. Cybercrimes can be committed from a remote location outside the affected state' boundaries which creates greater challenges to law enforcement authorities; it is not difficult to learn how to commit a particular cybercrime; its commission may require few resources in comparison to the potential damage it can cause; and, it is not often clearly illegal.[6]

There are no internationally unified definitions of computer crime, high technology crime, and cyber fraud as they have different meanings for criminal justice professionals around the world.[7] Therefore, instead of defining the cybercrime, the international or regional cybercrime instruments have listed several acts that per se constitute cybercrimes. For example, the Council of Europe's Convention on Cybercrime (Budapest Convention) considers the following acts as cybercrimes: offenses against the integrity, confidentiality and availability of computer data and systems which include illegal interception, illegal access, data interference, system interference, and misuse of devices; computer related forgery; computer related fraud; offenses related

[4] Abraham D. Sofaer & Seymour E. Goodman, *Cyber Crime and Security: The Transnational Dimension*, in THE TRANSNATIONAL DIMENSION OF CYBERCRIME AND TERRORISM 1, 1 (Abraham D. Sofaer & Seymour E. Goodman eds., 2001).
[5] Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* 10 Int'l J.L. & Info. Tech. 139, 144 (2002).
[6] *Id.* at 142.
[7] Marc Goodman, *International Dimensions of Cybercrime*, in CYBERCRIMES: A MULTIDISCIPLINARY ANALYSIS 311, 320 (Sumit Ghosh & Elliot Turrini eds., 2010).

to child pornography; and offenses related to infringements of copyright and related rights.[8]

The Arab Convention on Combating Information Technology Offenses (Arab Convention) provides for a wider range of crimes than the Budapest Convention. It includes offense of illicit access; offense of illicit interception; offense against the integrity of data; offense of misuse of information technology means; offenses committed by means of information technology to include forgery, fraud, pornography and those offences related to terrorism, organized crime, copyright and adjacent Rights; and illicit use of electronic payment tools.[9]

In fact, cybercrime knows no boundaries due to the architecture of the Internet which allows the data to be transmitted all over the world in just few seconds without any relevant obstacles or barriers. Therefore, it involves a transnational dimension as the perpetrator can cause extensive harm to numerous victims in different countries without leaving home.[10] In addition, there is difficulty in deciding where the cybercrime actually takes place.[11] That is because the current digital technologies allow the perpetrator of cybercrime to be anonymous as he/she can create an email account by providing false data, use several complicated Internet applications to alter the actual IP address, and benefit from encryption technology to hide any traces of the crime. All of these challenges make the tracing of cybercrime very difficult and time consuming for law enforcement authorities.[12]

As a result of, such special characteristics of cybercrime oblige states all over the world to depend upon each other in fighting against this serious crime. Therefore, it is a must to enhance all forms of international cooperation between states through the effective response to the mutual legal assistance and extradition requests. That is because such

---

[8] Council of Europe, Convention on Cybercrime 4-8, Nov. 23, 2001, E.T.S No. 185 (entered into force Jul. 1, 2004).
[9] League of Arab States, Arab Convention on Combating Information Technology Offenses 5-9, Dec. 21, 2010 (entered into force Feb. 7, 2014), http://www.lasportal.org/ar/legalnetwork/Documents/الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.pdf.
[10] Marc Goodman, *supra* note 7, at 315.
[11] Jean-Baptiste Maillart, *The limits of subjective territorial jurisdiction in the context of cybercrime,* ERA F. 1, 4 (2018).
[12] Jonathan Clough, *Cybercrime*, 37 Commw. L. Bull. 671, 673 (2011).

effective and rapid international cooperation is urgently required in order to smoothly collect the evidence from another jurisdiction for the purpose of conducting an efficient prosecution or to apprehend the offender who exists in a foreign country.[13]

The transnational dimension of cybercrime has encouraged the drafters of international instruments and national laws to adopt an expansive approach for asserting jurisdiction over cybercrime with the aim of combatting this crime and ensuring that there is no safe havens for criminals.[14] As a result, jurisdiction over cybercrime can be established based on several bases including territorial, active nationality, passive nationality, and protective principles.

However, such a broad approach can lead to situations whereby more than one country may claim jurisdiction over the same cybercrime which results in the dilemma of positive conflict over jurisdiction. This conflict may lead to several practical problems as it may hinder the mechanism of effective international cooperation in fighting against cybercrime, the violation of the fundamental principle of *ne bis in idem,* and the duplication of efforts by law enforcement officials of the involved countries.

This study explores the different approaches for managing the conflict of criminal jurisdiction over cybercrime with the aim of comparing the advantages and disadvantages of each approach. It argues that the most effective solution to this dilemma is to determine certain factors to be considered and evaluated by a body established for such a purpose or by the concerned states themselves in order to decide which country will take the exclusive competence over the cybercrime in accordance with the facts of each individual case and taking into account the characteristics of cybercrime. Establishment of these factors should reflect the interests of the different stakeholders related to cybercrime that includes like other crimes the interest of victim(s), criminal(s), and concerned states.

As long as it is accepted internationally that the jurisdiction over cybercrime can be established based on territory, active and passive personality, as well as the protective

[13] Marc D. Goodman & Susan W. Brenner, *supra* note 5*,* at 185.
[14] Jonathan Clough, *supra* note 12*,* at 678.

principles, the suggested factors should also include the interests of the state where the crime is committed, the state of the offender's nationality, the state of the victim's nationality, and the state whose vital interests have been affected by the crime. In addition, these factors should contain the interest of criminal proceedings as it is a must to achieve the interests of all the stakeholders.

In my opinion, these factors should not be given equal weight as many factors may be more relevant than others in light of the cybercrime' particularities and the decision in this regard should be reached on the basis of an aggregate balance of all these factors. I contend that such proposed solution is better than the attempt to solve such conflict through negotiation between the concerned states without providing them with concrete factors to be considered in reaching a decision in this regard.

Chapter two of this study explains the main characteristics of cybercrime which include its transnational nature and the possibility to be committed "nowhere and everywhere". Chapter three presents the different types of international cooperation to include the police and judicial cooperation and the main forms of the latter containing the extradition and mutual legal assistance requests as well as the international and national efforts to enhance such cooperation against cybercrime.

Chapter four details the different bases for exercising the criminal jurisdiction to include the territorial, active and passive personality, protective, and universality principles as well as their weight in the contemporary international law and how the main characteristics of cybercrime encourage for adopting an expansive approach toward jurisdiction over cybercrime which may result in the positive conflict of several jurisdictions.

Finally, chapter five discusses in detail the different approaches for resolving the dilemma of concurrent jurisdictional claims between more than one country over the same cybercrime and illustrates the advantages and disadvantages of each view. Then, it argues that there are certain factors which should be considered and evaluated in order to reach an adequate decision to solve such a conflict. This factors should include the interest of victim(s), the interest of the perpetrator(s), the interest of the state where the crime was committed, the interest of the state of offender's nationality, the interest of

the state of victim's nationality, the interest of the state whose one of its vital interests has been affected by the crime, and the interest of criminal proceedings.

II. Fundamental Characteristics of Cybercrime

Generally, there are two notable features of cybercrime including its transnational nature and it can be "nowhere and everywhere". This chapter details the meaning, the reasons behind, and different types of cybercrime that have this a cross-border dimension as well as several examples of case law that reflect such a character. In addition, it demonstrates how such feature creates obstacles for law enforcement authorities and challenges the traditional conceptualizations of criminal jurisdiction which has encouraged the adoption of a broad approach of jurisdiction over cybercrime. Then, this chapter shows the difficulty in determining the location where the cybercrime originates from, the means used by the offender to hide his/her location when committing this crime using examples from case law. It also illustrates how this character poses many difficulties for law enforcement authorities in the world.

A. Transnational Character of Cybercrime

Transnational crime is defined by the Ninth United Nation Congress on the Prevention of Crime and the Treatment of the Offenders as "offences whose inception, prevention and/or direct or indirect effects involved more than one country."[15] This congress considered computer crime as one of eighteen categories of transnational crime.[16]

According to Article (3/2) of the United Nations Convention against Transnational Organized Crime, "an offence 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".[17]

---

[15] The Ninth United Nation Congress on the Prevention of Crime and the Treatment of the Offenders, interim report by the secretariat 4 (April 1995), https://www.unodc.org/documents/congress/Previous_Congresses/9th_Congress_1995/017_ACONF.169.15.ADD.1_Interim_Report_Strengthening_the_Rule_of_Law.pdf.

[16] *Id.* at 12.

[17] United Nations Convention against Transnational Organized Crime 6, Nov. 15, 2000, 2225 U.N.T.S 209 (entered into force Sep. 29, 2003).

Cybercrime is covered by this Convention if it is committed by an organized criminal group as defined in Article (2/a) of the Convention[18] and involves more than one country in its commission, perpetration, planning, direct or indirect effects, or the activities of the criminal group. As a result of being subject to this Convention, the effective rules in relation to international cooperation between states included in this convention can be applied to the cybercrime of concern. This convention can also be used as a legal basis for such cooperation between the concerned states.

In most cases, cybercrime involves a transnational dimension because of the interconnected nature of the global networks allows the offender in one country to easily commit a cybercrime from his/her location which may affect victims in several countries.[19] As Paul Schiff Berman explains "in an electronically connected world the effects of any given action may immediately be felt elsewhere with no relationship to physical geography at all."[20] The transnational cybercrime may be committed by a non-state entity or by a governmental institution and may negatively affect individuals, corporations, governmental entities, non-governmental organizations, or other entities.[21]

There are several factors that effectively encourage criminals to commit a transnational cybercrime. The first factor is that the global target pool of computers and users of the internet which allows perpetrator to cause great harm to victims in other countries with no more effort than would be required to commit the crime in their own countries. The second factor is the widespread differences between countries in the legal, regulatory, or policy framework regarding cybercrime which affects negatively the efforts against this crime.[22] Such differences are due to several reasons including the absence of one unified and worldwide definition of cybercrime.[23] Also, the different approaches toward

---

[18] *Id.* at 5.
[19] Ellen S. Podgor, *Cybercrime: National, Transnational, or International,* 50 Wayne L. Rev. 97, 97 (2004).
[20] PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS 92 (2012).
[21] Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 Yale J. Int'l L. 191, 196 (2018).
[22] Abraham D. Sofaer & Seymour E. Goodman, *supra* note 4, at 6.
[23] Ales Zavrsnik, *Cybercrime Definitional Challenges and Criminological Particularities*, 2 Masaryk U. J.L. & Tech. 1, 10 (2008).

the control of the Internet i.e. whether the Internet should be controlled by itself or the government should interfere through certain procedures to protect the people from cybercrime such as the surveillance or blocking access to certain suspicious websites and what is the limit of such interference.[24]

The third factor is the need for effective international cooperation between the concerned states in investigating and prosecuting this crime especially in relation to mutual legal assistance which will be discussed later at the next chapter.[25] The fourth factor is the vulnerability of the existing computer programs that can be exploited by criminals because the designers of such software programs concentrate primarily on making their use much easier and consider the reliability and security as secondary issues.[26]

As stated in the introduction,[27] a cybercrime can be a computer crime or a computer related crime. Most often, the computer crime has a cross-border nature. The two common examples are infectious malware and denial-of-service (DoS). The first is a code designed to cause damage to data, networks or hosts when a user downloads an infected attachment from an Email's message or accesses a corrupt website.[28] There are different forms of this malware to include viruses, worms, trojans, ransomware, adware, spyware, malvertising, file-less malware, and hybrid form.[29] Whereas, the DoS is a barrage of fake requests from a single source launched by a perpetrator which overwhelm the intended computer system, network or server. Unlike malware which alters the functionality of the system, DoS attacks temporarily deny access to the target system. Malware and DoS could be merged to produce a distributed denial-of-service (DDoS) attack.[30]

---

[24] Soumyo D. Moitra, *Developing Policies for Cybercrime - Some Empirical Issues,* 13 Eur. J. Crime Crim. L. & Crim. Just. 435, 441-42 (2005).
[25] *See* discussion *infra* notes 72-74.
[26] Abraham D. Sofaer & Seymour E. Goodman, *supra* note 4, at 19-20.
[27] *See* discussion *supra* note 5.
[28] Alexandra Perloff-Giles, *supra* note 21, at 197.
[29] Rogar A. Grimes, 9 types of malware and how to recognize them, CSO FROM IDG (May. 1, 2019, 6:32 AM), https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html.
[30] Alexandra Perloff-Giles, *supra* note 21, at 197.

Likewise, conventional crimes that committed by means of computer that are called computer-related crimes can have a transnational dimension. Examples include forgery, stalking, and child pornography. For example, at 2002, German police investigation lead to the synchronous execution of thirty-seven search warrants in ten countries on members of a private Internet group exchanging and downloading child pornography on the Internet.[31]

Furthermore, the rapid development of digital technology in the form of cell phones and other devices results in several forms of digital evidence extracted from these devices can be used to prove ordinary offences.[32] In the meantime, sophisticated criminal groups benefit from the Internet in the commission of different transnational organized crimes such as the human trafficking, smuggling of migrants, and money laundering. In reality, this occurs through the taking of advantage of Internet technologies to be untraceable by law enforcement authorities.[33]

Indeed, there are many examples of case law that reflect the transnational nature of cybercrime. One of the most famous cases is the *Love Bug virus*,[34] which spread around the world in May 2000 and led to the shutting down of business and government computers in over forty-five countries resulting in damages of many billions of dollars. Later, this crime was attributed to someone in the Philippines which did not have a cybercrime law at this time. Because of that, the act was not illegal in the Philippines and the perpetrator did not subject to prosecution in this state which also refused extradition request from other countries because of the absence of dual criminality as a primary condition for extradition. As a result, this person was not prosecuted by any state.

[31] Peter Grabosky*, The Global Dimension of Cybercrime,* 6 *Global Crime* 146, 147 (2004).
[32] Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millenium*, 9 DUKE J. COMP. & INT'L L. 451, 455 (1999).
[33] *See* discussion *infra* note 43.
[34] Susan W. Brenner & Joseph J. IV Schwerha*, Cybercrime Havens Challenges and Solutions*, 17 Bus. L. Today 49, 49 (2007).

Another example of such cross-border dimension of cybercrime is the *Vladimir L.Levin case*.[35] A group of Russian computer hackers attempted to steal about 10.7 million Dollars from Citibank customers' accounts in the USA by manipulating its computerized fund transfer system. In this case, L.Levin gained access over forty times to Citibank's fund transfer system using stolen account identification numbers and passwords and authorized the transfer of funds from Citibank's head office in New Jersey to accounts which Levin and his co-conspirators had in several countries by using a computer terminal in his employer's office in St Petersburg. After that, an arrest warrant was issued by a US court but his extradition was rejected because there was no treaty for extradition at this time between the USA and Russia. Later, Levin was arrested in England and extradited to the USA based on the extradition treaty between them.

At 2003, the information gathered for the United Nation Office on Drugs and Crime's Comprehensive study showed that the percentage of cybercrime acts that involve a transnational dimension was around 70% in Europe, 50% in Asia and Oceania, 40% in Africa, and 30% in the Americas.[36] Conversely, cybercrime can be a local one which adjusts to the traditional model of crime if its commission takes place entirely within the territory of one state i.e. the victim and perpetrator physically exist in the territory of the same country where the crime is committed.[37] One example is the illegal access to a company's computer system for the purpose of stealing a sensitive information from the hard disk.

In fact, this transnational dimension of cybercrime creates new opportunities for criminals which imposes great technical and legal challenges for the local law enforcement authorities in investigating and prosecuting this crime regarding the collection of evidence and apprehension of criminals.[38] Also, it challenges the traditional conceptualization of criminal jurisdiction as the criminal act no longer necessarily takes place wholly within the territory of one state.[39] Thus, this

[35] Ikenga K.E. Oraegbunam, *Towards Containing the Jurisdictional Problems in Prosecuting Cybercrimes: Case Reviews and Responses*, 7 Nnamdi Azikiwe U. J. Int'l L. & Juris. 26, 27 (2016).
[36] Comprehensive Study on Cybercrime, *supra* note 2, at 183.
[37] Susan W. Brenner, *Cybercrime jurisdiction*, 46 Crime, L. and SOC. Change 189, 193 (2006).
[38] Marc D. Goodman & Susan W. Brenner, *supra* note 5, at 142.
[39] Susan W. Brenner, *supra* note 37, at 190.

extraterritorial nature has encouraged the drafters of domestic laws and international and regional cybercrime instruments to adopt an expanded approach in relation to jurisdiction over cybercrime which may lead to the situation of positive conflict of criminal jurisdiction over the same cybercrime between two or more countries and this point will be discussed later in detail at chapter four of this study.[40]

In sum, there are no borders on the Internet as the cyberspace makes sovereign boundaries and physical space irrelevant. In fact, the perpetrator only needs a computer and an Internet connection to commit a cybercrime that can affect a several victims in other countries which destroys the conventional jurisdictional realms of sovereign states.

B. Cybercrime Could be "Nowhere and Everywhere"

The traditional crime is usually linked to a geographic location where the crime was committed and the criminal is physically existing at the crime scene. Therefore, law enforcement officials can apprehend the offender and bring him/her to justice. Whereas, cybercrime frequently is not clearly linked to any geographic location as it can be committed from any location with Internet access. Also, in many situations, it is difficult to determine where the cybercrime originates from. It may appear to have been committed in a certain country but actually originates elsewhere and having been routed through several jurisdictions before reaching its "last address".[41]

In fact, any action on the Internet can be attributed to a single user through identifying the IP address which pinpoints the specific network and device being used for accessing the Internet and identifies its location. An IP address can be static assigned on a permanent basis as in the case of website address or dynamic temporarily assigned for the duration of an online session from a pool of addresses available to an Internet Service Provider.[42] Nevertheless, the perpetrator of such a crime can easily hide his/her location with anonymizing services that make the task of the identification by the law enforcement extremely difficult. Indeed, there are several digital technologies available

[40] *See* discussion *infra* note 178.
[41] Peter Grabosky*, supra* note 31, at 150.
[42] United Nation Office on Drugs and Crime, *The use of the Internet for terrorist purposes,* 62 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

online that facilitate the anonymity on the Internet. They are used by the criminals to hide their IP address or change it in order to be untraceable by the law enforcement authorities such as VPN software that allows the user to change his/her IP address to another fake one and browse the web anonymously.[43]

An example that proves the difficulty in determining where the cybercrime originates from is a case of a cybercrime committed in Hong Kong. In this case the evidence collected in an investigation initiated by Hong Kong police upon a complaint from a local woman who had been a victim of a cyber-stalker linked to a system in Colorado proved that the perpetrator resides in Hong Kong. Whereas, the offending communications seemed falsely to be routed through a server in Colorado.[44] Another instance that confirms such difficulty is the extensive cyber-attack against several governmental institutions in the USA and South Korea at July 2009. Initially, the South Korean government believed that this attack had been committed from North Korea. Later, security experts suggested that this attack may have operated from the United Kingdom and not North Korea.[45]

In fact, such challenges in identifying the perpetrator of a cybercrime and his/her location due to the use of digital technologies have posed many difficulties for the law enforcement authorities in the investigation and prosecution process of this crime. Hence, those authorities are obliged to be well-informed of rapidly developing technologies which requires advanced training in new investigative techniques and the use of highly developed technologies to detect the criminal and bring him/her to justice.[46]

In sum, this chapter has shown the fundamental characteristics of cybercrime to include its transnational nature and the possibility of being "nowhere and everywhere". The next chapter details the two types of international cooperation including police and

---

[43] Rob Mardisalu, *How to Hide my IP Address* (March 2019), https://thebestvpn.com/hide-ip/
[44] Peter Grabosky, *supra* note 31, at 150-51.
[45] Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 Vand. J. Transnat'l L. 57, 60 (2010).
[46] P.N. Grabosky, *Crime in Cyberspace*: in COMBATING TRANSNATIONAL CRIME 195, 203 (Phil Williams & Dimitri Vlassis eds., 2001).

judicial cooperation as well as the main forms of the latter to include the extradition and mutual legal assistance requests.

III. International Cooperation against Cybercrime

In reality, the transnational nature of cybercrime and the difficulty in identifying the perpetrator or the place of the crime's commission have created several obstacles and challenges for law enforcement authorities around the world in relation to the obtaining of cross-border evidence and extradition of criminals. Thus, the effective, rapid, and well-functioning international cooperation between states on criminal matters is essential in enhancing the investigation and prosecution proceedings of cybercrime that is facilitated globally and has negative consequences in different states.[47] This chapter looks at the two types of international cooperation which are police and judicial international cooperation. Then, it highlights the most common forms of the judicial one to include extradition and mutual legal assistance requests. After that, it illustrates the international and national efforts to enhance such cooperation against cybercrime.

A. Police International Cooperation

Police international cooperation is the exchange of data and information between police authorities of different countries with the aim of sharing criminal intelligence, conducting investigation, and apprehending suspects.[48] Such exchange can be done either directly or through one of the inter-governmental organizations such as the International Criminal Police Organization (INTERPOL) and European Police Office (EUROPOL) for the purpose of combatting different kinds of crimes.

1. International Criminal Police Organization (INTERPOL)

INTERPOL is an inter-governmental organization which has in its membership 194 countries with the aim of allowing the police authorities in all member states to share and access data on crimes and criminals as well as providing them with a wide range of technical and operational supports in order to achieve the security of the world.[49]

---

[47] Pedro Verdelho, *the effectiveness of international co-operation against cybercrime: examples of good practices* 1, 4 (2008), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3a2.

[48] FREDERIC LEMIEUX, INTERNATIONAL POLICE COOPERATION: EMERGING ISSUES, THEORY AND PRACTICE 1 (2d ed. 2013).

[49] What is Interpol, https://www.interpol.int/en/Who-we-are/What-is-INTERPOL.

One of the major functions of INTERPOL is to enhance international cooperation between law enforcement agencies to ensure the secure and fast exchange and analysis of information related to criminal activities and suspected persons. In fact, it achieves this role through the I-24/7 global police communication system which links law enforcements in all member countries and allows them to share police information in order to enhance the efficiency of criminal investigations.[50] Furthermore, this system can facilitate bilateral or multilateral police requests or the delivery of a formal legal assistance request from one central authority to another.[51]

The INTERPOL's cybercrime program is an important tool in this regard. That is because its purpose is to support the exchange of information among member states through regional working parties and conferences, assist and coordinate international operations, and offer training courses to develop and enhance professional standards. In addition, it plays an important role in creating a worldwide list of contact officers for cybercrime investigations for the purpose of assisting member countries in the event of cyberattacks, identifying emerging threats and sharing this intelligence with member states, providing a secure web portal for accessing operational information and documents, and developing strategic partnerships with other international organizations and private sector institutions.[52]

2. European Police Office "EUROPOL"

Unlike INTERPOL which composes members from countries around the world, EUROPOL is the European union' law enforcement agency with the main target of maintaining security on Europe for the benefit of all EU citizens.[53] The main mandate of Europol is to promote the effectiveness of cooperation between the law enforcement authorities of EU member states in preventing and fighting terrorism and other forms of transnational organized crime. Also, it has a fundamental role in the European Cybercrime Task Force which is a group of experts from Europol, Eurojust, and the European Commission with a mandate to work together with the heads of European

[50] The use of the Internet for terrorist purposes, *supra* note 42, at 79-80.
[51] Comprehensive Study on Cybercrime, *supra* note 2, at 187.
[52] The use of the Internet for terrorist purposes, *supra* note 42, at 80.
[53]ABOUT EUROPOL, https://www.europol.europa.eu/about-europol.

Union cybercrime units in order to enhance transnational combating against cybercrime.[54]

In 2013, Europol set up the European Cybercrime Centre (EC3) to support the response of law enforcement authorities to cybercrime in the EU with the aim of protecting European citizens, businesses and governments. In reality, this center has played an important role in the fight against cybercrime as it serves as the central hub for criminal information and intelligence and has offered highly specialized technical and digital forensic support capabilities to investigations and operations. As a result, it has been involved in several high-profile operations and on the spot operational support deployments which have led to hundreds of arrests as well as it has analyzed very large number of files. Moreover, the EC3 issues yearly the Internet Organized Crime Threat Assessment "IOCTA" on key results and emerging developments and threats in cybercrime.[55]

B. International Judicial Cooperation

Besides the police international cooperation, the international judicial cooperation between the judicial authorities of different countries is essential in countering cybercrime. Traditionally, the legal basis for such cooperation against cybercrime can be one of the binding international or regional instruments such as the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information,[56] the Budapest Convention,[57] the Arab Convention,[58] the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security,[59] or a bilateral agreement or the principle of reciprocity which is a promise that the requesting state will provide the requested state with the same type of assistance in the future.[60]

---

[54] The use of the Internet for terrorist purposes, *supra* note 42, at 80-8.
[55]EUROPEAN CYBERCRIME CENTRE – EC3, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
[56] The commonwealth of Independent States, Agreement on Cooperation in Combating Offences related to Computer Information, June 1, 2001 (entered into force Mar. 14, 2002).
[57] Convention on Cybercrime, *Surpa* note 8.
[58] Arab Convention on Combating Information Technology Offenses, *supra* note 9.
[59] The shanghai Cooperation Organization, Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, June. 16, 2009 (entered into force Jan. 5, 2012).
[60] Comprehensive Study on Cybercrime, *supra* note 2, at 201.

In fact, the extradition and mutual legal assistance requests are the most important formal mechanisms of international judicial cooperation against cybercrime. Other forms of cooperation such as transfer of criminal proceedings or prisoners, asset recovery and confiscation of criminal proceeds are less relevant in practice.[61]

1. Extradition

One of the most important forms of international judicial cooperation is the extradition which is defined by Model Law as the surrender of any person who is sought by the requesting state to subject to a criminal prosecution, to stand a trial, or to serve a sentence for an extraditable offence.[62] The precondition for the acceptance of an extradition request is dual criminality which means that the act must be a crime in both laws of the requesting and requested states. However, it is not required that the underlying activity be punishable with the same type of legal provision.[63]

Also, the crime which is the subject of an extradition request should be an offence for which the laws of the concerned states allow extradition. In reality, the determination of what constitutes an extraditable offence is made through a treaty which decides the offences for which extradition may be allowed or by the seriousness of the penalty that may be imposed by the national law.[64] For example, Article (24/a) of the Budapest Convention provides that "this Article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty".[65]

---

[61] Marco Gercke, UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE 267 (2012).
[62] Model Law on Extradition 8 (2004), https://www.unodc.org/pdf/model_law_extradition.pdf.
[63] Comprehensive Study on Cybercrime, *supra* note 2, at 60.
[64] United Nation Office on Drugs and Crime, Manual on Mutual Legal Assistance and Extradition 45-46 (September 2012), https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf.
[65] Convention on Cybercrime, *supra* note 8, at 14.

In fact, there are several bases for the refusal of an extradition request which differ from one convention to another. According to chapter two of the Model Law on Extradition, the extradition request may be rejected in the following circumstances:[66]

- If the offence has a political nature. Nevertheless, the model law excludes certain acts from being considered as political offence such as murder, inflicting serious bodily harm, and kidnapping.
- If there are substantial grounds to believe that such request has been sent for the purpose of prosecuting or punishing the person sought on account of his/her race, ethnic origin, nationality, religion, political opinions, sex or status.
- If the person sought has been or would be subjected in the requesting state to cruel, or torture, degrading or inhuman treatment or punishment or will not receive the minimum fair trial guarantees in the criminal proceedings in the requesting country.
- If there has been a final judgement rendered and enforced against the person in relation to the offence for which extradition is requested or the prosecution or punishment against the person sought is barred by lapse of time, prescription or statute of limitation at the time of receiving the request for extradition.
- If the act is an offence under military law which is not also a crime under ordinary criminal code in the requesting country or if the punishment for the offence is the death penalty under the law of the requesting country and is not so punishable according to the law of the requested state, unless the competent authorities of the requesting country submit sufficient assurances that this penalty will not be imposed or, if so, will not be carried out.
- If the person sought is a national of the requested state provided that it will refer the case without delay to the competent prosecution authority which is called as the principle of *aut dedere aut judicare* (extradite or prosecute).

2. Mutual Legal Assistance

In addition to the extradition, there is also the mutual legal assistance. It is a process by which the judicial authority in one state seeks and requests assistance from its counterpart in another state in gathering evidence to be used in criminal proceedings against a specific crime.[67] In fact, criminal proceedings are based on evidence which

[66] Model Law on Extradition, *supra* note 62, at 12-25.
[67] Manual on Mutual Legal Assistance and Extradition, *surpa* note 64, at 19.

increasingly is existed outside of the state' borders. Thus, there is now an increased assertion on the international level for the need to develop effective instruments that can facilitate assistance with cross border evidence gathering.[68]

There are several grounds for the refusal of mutual legal assistance as shown in Article (3) of the Revised Manuals on the Model Treaty on Extradition and on the Model Treaty on Mutual Assistance in Criminal Matters. These grounds include if the requested state believes that the request, if granted, would prejudice its sovereignty, security, public order or other essential public interests; regards the offence as being of a political nature; or has substantial grounds to believe that the request has been made for prosecuting a person on account of his/her race, sex, religion, nationality, ethnic origin or political opinions. Other reasons include if the request relates to an offence whose prosecution in the requesting state would be incompatible with the requested state's law on double jeopardy; requires the requested state to carry out compulsory measures that would be inconsistent with its law; or the act is an offence under military law which is not an offence under ordinary criminal law.[69]

In fact, there are many forms of mutual legal assistance as illustrated in Article (18/3) of the United Nations Convention Against Transnational Organized Crime such as the taking of a statement from a person, the production of a document, and the execution of search, seizure, and freezing orders.[70] Regarding cybercrime, the forms of requested assistance are listed in the Budapest Convention in Articles (29) to (34) which include expedited preservation of stored computer data, expedited disclosure of preserved traffic data, the search, seizure, and disclosure of stored computer data, the real-time collection of traffic data, the interception of content data, and the access to stored computer data with consent or where publicly available.[71]

In reality, the traditional regime for mutual legal assistance imposes many difficulties on the investigations related to cybercrime because the implementation of such a request

---

[68] Revised Manuals on the Model Treaty on Extradition and on the Model Treaty on Mutual Assistance in Criminal Matters 66, https://www.unodc.org/pdf/model_treaty_extradition_revised_manual.pdf.
[69] *Id*. at 86.
[70] United Nations Convention against Transnational Organized Crime, *supra* note 17, at 20.
[71] Convention on Cybercrime, *surpa* note 8, at 18-20.

requires time-consuming formal procedures.[72] Such a request and its response must be made rapidly in the urgent cases because computer data can be deleted very easily which makes it impossible to know the perpetrator or collect critical evidence. Also, many forms of computer data are stored for only a short time before being deleted. In other cases, significant harm to persons or property may occur if evidence is not gathered rapidly.[73] Thus, such a regime for mutual legal assistance should cope with the required speedy response in relation to a cybercrime's investigation.[74]

To such an effect, Article (25) of the Budapest Convention provides that "Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication".[75] Therefore, this article encourages the authorities of member states to benefit from the developed means of communication in sending or responding to a request for mutual assistance.

C. International and National Efforts to Enhance International Cooperation against Cybercrime

In reality, there are several efforts to promote international cooperation against cybercrime. At the international level, different international binding or non-binding instruments in relation to cybercrime confirm the importance of both police and judicial international cooperation. For example, chapter three of the Budapest Convention which sets up the general principles relating to international cooperation, extradition, mutual legal assistance, and the establishment of a twenty-four hour, seven-day-a-week network in order to ensure the application of immediate assistance for the purpose of ensuring effective investigation and prosecution proceedings against this crime.[76]

---

[72] Marco Gercke, *supra* note 61, at 106.
[73] Explanatory Report to the Convention on Cybercrime 44 (2001), https://rm.coe.int/16800cce5b.
[74] Marco Gercke, *supra* note 61, at 106.
[75] Convention on Cybercrime, *surpa* note 8, at 15.
[76] Convention on Cybercrime, *Surpa* note 8, at 14-21.

Also, at the national level, many domestic laws provide for international cooperation. For instance, Article (4) of the Egyptian Anti Information Technology Crimes Law No. 175 for the year 2018 (Egyptian Law) encourages the competent Egyptian authorities to cooperate with their counterparts in other countries in relation to the exchange of information in order to avoid the occurrence of cybercrime, facilitate their investigation, and achieve the tracking of perpetrators.[77]

Nevertheless, it is a must to better enhance international cooperation against cybercrime.[78] Indeed, one major way in this regard is to harmonize national laws in order to promote the mechanisms of mutual legal assistance and extradition.[79]

Generally, each country has its own culture, legal tradition, and historical background which affects its substantive and procedural laws. Therefore, the international response to cybercrime should attempt to accommodate these differences and achieve some degree of harmonisation between national substantive and procedural laws for the purpose of promoting international cooperation. Such harmonisation between substantive laws is urgent to ensure the criminalization of all forms of cybercrime in the different countries to eliminate the possibility of safe havens if the conduct is not a crime in a specific country which will not only hinder the domestic prosecution but also will impede the effective response to the extradition and mutual legal assistance requests due to the lack of dual criminality condition.[80]

Similarly, the consistency between procedural laws is also necessary to promote international cooperation through mutual legal assistance requests. Usually, the procedural law defines the powers of law enforcement authorities such as the competence to seize stored computer data, intercept content data or issue a production order, a search warrant of computer systems, or an order for the expedited preservation of stored computer data. In fact, a requested state can only provide assistance within its

---

[77] Law No. 175 of 2018 (Law of Anti-Information Technology Crimes), *Al-Jarida Al-Rasmiyya*, 14 Aug. 2018, No. 32 bis [c], pp. 3-25 (Egypt) [hereinafter Egyptian Anti-Information Technology Crimes Law].
[78] *See* discussion *supra* note 47.
[79] Comprehensive Study on Cybercrime, *supra* note 2, at 56.
[80] Jonathan Clough, *A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation*, 40 MONASH U. L. REV. 698, 700-01 (2014).

territory to the requesting country as long as the requested procedure can be taken by its national authority according to its procedural law. For example, if the requested country does not have the necessary procedural power for the expedited preservation of computer data, then it will refuse the request from the requesting state for such a measure through mutual legal assistance.[81]

In fact, the inherent transnational nature of cybercrime as illustrated in chapter two[82] increases the need for such harmonisation more than other crimes that may also have a transnational dimension such as the human trafficking, smuggling of drugs, and money laundering. However, this does not mean that all cybercrime laws should be identical but what is required is some degree of harmonisation that enables international cooperation mechanisms between law enforcement authorities to work effectively.[83]

Indeed, several international and supranational organizations to include, in particular, the United Nations, the Council of Europe, the European Union, the Organization for Economic Cooperation and Development, and INTERPOL have recognized the inherent cross-border nature of cybercrime which requires an international harmonization of legal, technical, and other solutions. These organizations indeed have a great impact in building international awareness and cooperation in this respect.[84]

Such efforts have resulted in the conclusion of several conventions including the Budapest Convention,[85] the African Union Convention on Cyber Security and Personal Data Protection,[86] the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information,[87] the Arab convention,[88] and the Shanghai Cooperation Organization Agreement on Cooperation

[81] Comprehensive Study on Cybercrime, *supra* note 2, at 61.
[82] *See* discussion *supra* note 19.
[83] Jonathan Clough, *supra* note 80, at 700-01.
[84] Marc D. Goodman & Susan W. Brenner, *supra* note 5, at 165.
[85] Convention on Cybercrime, *surpa* note 8.
[86] The African Union, African Union Convention on Cyber Security and Personal Data Protection, June. 27, 2014.
[87] Agreement on Cooperation in Combating Offences related to Computer Information, *surpa* note 56.
[88] Arab Convention on Combating Information Technology Offenses, *supra* note 9.

in the Field of International Information Security.[89] Moreover, several relevant United Nations system decisions, resolutions, and recommendations have been issued in this regard such as General Assembly Resolutions 55/63 of December 4, 2000 [90] and 56/121 of December 19, 2001 [91] on Combating the Criminal Misuse of Information Technologies. Nevertheless, there is still an imperative need for a global multilateral treaty for combating cybercrime that can accomplish the harmonization among national substantive and procedural laws.[92]

Besides the need for harmonization, there is an urgent necessity for an effective partnership between law enforcement authorities and Internet Service Providers (ISPs) in the private sector as they have played a crucial role in detecting, discovering, and proving the case against the offender(s) because the data is uploaded, transmitted or stored on their servers. Thus, such cooperation must secure the obtaining of valid data about the identification of offenders and their location.[93]

Indeed, one of the most important tools regarding this cooperation is the 2019 Practical Guide for Requesting Electronic Evidence Across Borders which was issued by the United Nation Office on Drugs and Crime. It explains how law enforcement authorities around the world can request digital evidence from ISPs as well as contains the policies of several ISPs that show the rules which govern their cooperation with law enforcement authorities around the world.[94] Nowadays, many ISPs accept the request for the preservation or emergency disclosure of data which comes directly from a foreign law enforcement authority without being transmitted through the competent national authority in the state where the ISP is located.[95]

---

[89] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, *surpa* note 59.
[90] G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Dec. 4, 2000).
[91] G.A. Res. 56/121, U.N. Doc. A/RES/56/121 (Dec. 19, 2001).
[92] Ikenga K.E. Oraegbunam, *surpa* note 35*,* at 40.
[93] Cristos Velasco, *Cybercrime jurisdiction: past, present and future,* 16 ERA F. 331, 340 (2015).
[94] United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html.
[95] Information for Law Enforcement Authorities, https://www.facebook.com/safety/groups/law/guidelines/.

In addition, the national role is very important to support such international efforts as each state should establish a national well-specialized entity to deal with transnational issues of cybercrime and cooperate effectively with its counterparts throughout the world through the different forms of international cooperation.[96] Furthermore, every state should develop its national laws, strategies, authorities, and abilities in the fight against cybercrime. The well-organized cooperation with the private sector and civil society at the national level and the coordination between the roles and efforts of governmental institutions are essential factors in countering cybercrime.[97]

In sum, this chapter has shown the different forms of international cooperation against transnational cybercrime as well as the international and national efforts to promote such cooperation. The next chapter explains the different grounds for asserting criminal jurisdiction. Then, it illustrates how cybercrime characteristics have encouraged the application of an expansive approach in relation to jurisdiction over cybercrime which may lead to the situation of a positive conflict of jurisdiction.

[96] Abraham D. Sofaer & Seymour E. Goodman, *supra* note 4, at 3.
[97] David Satola & Henry L. Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*, 37 Wm. Mitchell L. Rev. 1745, 1788 (2011).

IV. Jurisdiction over Cybercrime

Actually, the exercise of criminal jurisdiction can be based on several grounds including territoriality, active personality, passive personality, protective, and universality principles that could lead to the situation of conflict of jurisdiction between states. This chapter starts with discussing in detail those different bases for the assertion of jurisdiction and their weight in the contemporary international law. Then, it shows how the features of cybercrime have led to the adoption of a broad approach to the exercise of jurisdiction which may result in the concurrent jurisdictional claims over the same cybercrime.

A. Jurisdiction in International Law

Traditionally, jurisdiction in international law is a central feature of principles of state sovereignty and equality of states. It can be defined as the power of a sovereign state to regulate or otherwise impact people, properties, and circumstances whether by legislation, executive decree, or the court's judgment.[98]

Historically, jurisdiction has been understood in reference to geographical borders since the emergence of the sovereign nation state and the exercise of jurisdiction over crimes occurring outside the state's territory was seen as an exception to the rule. However, the late twentieth and early twenty-first century has seen a dramatic rise in the commission of transnational organized crimes such as terrorism, cybercrime, and human trafficking. Hence, countries have become interested in criminal activity occurring outside their territory either because of the inability or unwillingness of another state to prosecute such serious crimes, or because it achieved some sort of domestic or foreign policy agenda. As a result, the international community has concluded several treaties that either require or allow extraterritorial jurisdiction over some types of criminal offences,[99] as shown later in relation to cybercrime.[100]

In general, under the customary international law, the territorial principle is regarded as the basic principle of jurisdiction. Nevertheless, it is also accepted that national law may

---

[98] MALCOLM N. SHAW, INTERNATIONAL LAW 483 (8th ed. 2017).
[99] DANIELLE IRRELAND-PIPER, ACCOUNTABILITY IN EXTRATERRITORIALITY: A COMPARATIVE AND INTERNATIONAL LAW PERSPECTIVE 3 (2017).
[100] *See* discussion *infra* notes 179, 180.

extend its jurisdiction over conduct that is committed outside the state's physical territory based on one of the recognized principles of extraterritorial jurisdiction: the active personality, passive personality, protective, and universality principles.[101]

1. Territorial Principle

The first ground for criminal jurisdiction is the territorial principle which is based on the location of a crime's commission. Traditionally, this principle is the most common basis of jurisdiction over crimes and the countries impose their jurisdiction over the offenses committed in whole or in part within their territory.[102] This principle is derived from state sovereignty and universally recognized without raising any controversy.[103]

In fact, this principle depends on the absolute right of every state to impose its jurisdiction over all acts committed within its territory whether criminal or not as well as over all persons existing in such territory whether on land, sea, or the airspace above the land and sea territory.[104] National criminal law is territorial in essence and based on the conception of law enforcement as a mean of keeping the peace and security within a state's territory.[105]

Nevertheless, it is argued that the territorial doctrine has lost its primacy as the most common base for asserting jurisdiction due to several reasons. The first reason is that the contemporary developments in the era of international cooperation in criminal matters between states allow the conviction of an accused person for a crime committed outside state's territory through the gathering of evidence from different foreign jurisdictions. Such developments undermine the argument that the territorial principle supports the common law principle of confrontation in criminal cases by ensuring that

---

[101] CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 101 (2d ed. 2015); *see also* DANIELLE IRRELAND-PIPER, *supra* note 99, at 2-3.
[102] Ray August, *International Cyber-Jurisdiction: A Comparative Analysis,* 39 Am. Bus. L.J. 531, 536 (2002).
[103] ALINA KACZOROWSKA-IRELAND, PUBLIC INTERNATIONAL LAW 358 (5th ed. 2015).
[104] ANDERS HENRIKSEN, INTERNATIONAL LAW 85 (2d ed. 2019).
[105] Christopher L. Blakesley, *United States Jurisdiction over Extraterritorial Crime,* 73 J. Crim. L. & Criminology 1109, 1114 (1982).

the perpetrator will be tried in the place of the crime's commission where witnesses and evidence are more readily available.[106]

The second reason is the sharp increase in the number of transnational crimes which pushes states to adopt several grounds to assert their jurisdiction in order to establish the criminal liability of the offenders according to their national laws.[107] The third one is that the territorial borders between states have become less relevant, especially within the European Union where EU's citizens are entitled by law to move easily within many countries without the need for the ordinary requirements such as a passport or Visa.[108]

In reality, the application of the territorial principle may cause a practical problem when a crime is initiated or planned in one state but committed in another one. In fact, the international law has evolved two approaches to solve this dilemma which are the objective and subjective territorialities. The first one is based on the effect of the crime and emphasizes that a state will have jurisdiction over the crime that was executed on its territory even though some of its elements occurred abroad. The second one, which is of a great importance in countering the transnational crime like cybercrime, holds that a state has jurisdiction over all acts that are completed abroad as long as they are initiated or planned on its territory.[109]

Relating to cybercrime, the national cybercrime laws impose their jurisdiction when all or part of the *modus operandi* of the offence occurs in the state territory. Also, at the international level, Article (22) of the Budapest Convention adopts the territorial doctrine as the primary basis for asserting jurisdiction over cybercrime.[110] Later, the weight of territorial jurisdictional claim in relation to cybercrime will be assessed separately in chapter five.[111]

---

[106] P. Arnell, *The Case for Nationality Based Jurisdiction,* 50 INT'L & COMP. L.Q. 955, 958-59 (2001).
[107] *See* discussion *supra* note 99.
[108] P. Arnell, *supra* note 106, at 959.
[109] ANDERS HENRIKSEN, *supra* note 104, at 85-86.
[110] Convention on Cybercrime, *surpa* note 8, at 13.
[111] S*ee* discussion *infra* notes 249-254.

Actually, the application of the territorial principle in relation to cybercrime raises a very critical debate regarding whether the location of the cybercrime is the place of download, the place(s) of uploading or the place(s) through which the data is transported. For example, in *LICRA V. Yahoo!*,[112] two civil organizations sued Yahoo, an American online service provider, in France for showing Nazi propaganda, memorabilia and objects available for purchase in the Yahoo French website which was illegal in France. The Tribunal de Grande Instance of Paris asserted its jurisdiction over Yahoo because the memorabilia and objects were available to residents located in France even though the data could also be uploaded from a place outside France and stored in Yahoo servers in the USA. Then, the Tribunal de Grande Instance of Paris ordered Yahoo to remove such content and destroy all the concerned files stored in its server. Therefore, this court considered the place of data download as the base for exercising the territorial jurisdiction over the involved cybercrime.

2. Active Nationality Principle

The second ground for asserting jurisdiction is the active nationality principle which is based on the nationality of the accused.[113] Indeed, it is universally accepted that a state may prosecute its own national who has committed a crime abroad.[114] States have an inherent right to apply its jurisdiction over their nationals even if all the elements of the crime were committed outside its territory.[115]

In fact, the application of this principle is justified on several reasons. First, it is important to prevent the state's national from circumventing his/her state's law that forbids certain acts by committing them in other countries where such acts are legal.[116] Second, it is recognized that a sovereign state may legitimately impose obligations on its subjects because nationality is considered as the link between the state and its people which establishes rights and duties between nationals and their state that gives the latter

[112] Armando A. Cottim, *Cybercrime, Cyber terrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime*, 2 Eur. J. Legal Stud. 55, 67-68 (2010).
[113] REBECCA M.M. WALLACE & OLGA MARTIN-ORTEGA, INTERNATIONAL LAW 124 (6th ed. 2009).
[114] ALINA KACZOROWSKA-IRELAND, *supra* note 103, at 360.
[115] MARTIN DIXON ET AL., CASES & MATERIALS ON INTERNATIONAL LAW 290 (6th ed. 2016).
[116] ADEMOLA ABASS, COMPLETE INTERNATIONAL LAW 536 (2012).

the right to assert jurisdiction over its nationals for acts committed inside or outside its territory.[117]

The third ground is the principle of allegiance which each person owes to his/her state of nationality that entitles this state to exercise its jurisdiction over the crime committed everywhere by this person.[118] Fourth, many states, especially civil law countries, do not extradite their own nationals who commit a crime abroad to the country where the crime was committed. Therefore, the asserting of jurisdiction by the state of nationality is needed to prevent the criminal from escaping prosecution.[119] In such cases, the territorial state may welcome the exercise of jurisdiction by the state of nationality to ensure the prosecution of the criminal. In this way, this principle may decrease rather than increase international conflict between states in such situation.[120]

In reality, active nationality principle is universally acknowledged. However, it is used more extensively by civil law than common law countries which restrict its application to the more serious crimes. For example, the UK's application of this principle is restricted to several serious crimes such as sexual offences and murder. Similarly, the USA limits its exercise to certain crimes such as drug trafficking, treason, and crimes by or against the armed forces.[121] One example of the application of the nationality principle is found in *R. V. Earl Russell*,[122] A national of the UK was convicted of bigamy although the second act of marriage took place outside the UK and the court asserted its jurisdiction based upon his British nationality. Thus, the court exercised its jurisdiction over the illegal act upon the existence of active nationality principle as a ground for asserting jurisdiction.

Sometimes, the state's law conditions the application of the nationality principle on the return of the offender to his/her state of nationality and the requirement that the act which was committed abroad is also criminalized according to the law of the country

---

[117] GIDEON BOAS, PUBLIC INTERNATIONAL LAW: CONTEMPORARY PRINCIPLES AND PERSPECTIVES 255 (2012).
[118] ALINA KACZOROWSKA-IRELAND, *supra* note 103, at 360.
[119] Zsuzsanna Deen-Racsmany, *The Nationality of the Offender and the Jurisdiction of the International Criminal Court*, 95 AM. J. INT'L L. 606, 609 (2001).
[120] CEDRIC RYNGAERT, *supra* note 101, at 106-07.
[121] REBECCA M.M. WALLACE & OLGA MARTIN-ORTEGA, *supra* note 113, at 124-25.
[122] ALINA KACZOROWSKA, PUBLIC INTERNATIONAL LAW 121 (2d ed. 2003).

where it occurred.[123] For example, Article (3) of the Egyptian Penal Code states that "any Egyptian committing abroad a deed considered to be a felony or misdemeanor under the present law, shall be liable to punishment by virtue of its provisions if he/she returns to the country and the deed is punishable by virtue of the law of the country where it is committed".[124]

Nevertheless, the exercise of the nationality principle may cause an overlap of jurisdiction between the state of a defendant's nationality and the territorial state where the crime was committed. In such case, the state of nationality will assert its jurisdiction because the offender holds its own nationality. Therefore, it will refuse the extradition based on the principle of *aut dedere aut judicare* which allows the state of nationality to refrain from extraditing its own national provided that it refers the case to its own competent authorities without delay. On the other hand, the territorial state will also claim its jurisdiction because it believes that it has the closest link to the crime which was committed in its own land where the witnesses, victims, and evidence exist. Thus, the exercise of jurisdiction is a sort of sovereignty over its own territory.[125] Indeed, this conflict needs to be resolved by obvious rules that will be discussed later in this study.[126]

One well-known example of such a conflict is the *Lockerbie case*.[127] In 1988, a plane, registered in the USA, exploded over Scotland which resulted in the killing of all passengers and crew as well as persons on the ground in the town of Lockerbie. The victims were of 21 different nationalities but mainly from the USA and UK. Later, two Libyan nationals were accused of planting the bomb on board the plane. Nevertheless, Libya refused their extradition due to their Libyan nationality and requested all related evidence to be used in its own judicial investigation based on Article (7) of Montreal Aircraft Sabotage Convention which established the principle of *aut dedere aut judicare*.[128] While, the USA and the UK primarily claimed their jurisdiction based upon

---

[123] ADEMOLA ABASS, *supra* note 116*,* at 536.
[124] Law No. 58 of 1997 (criminal code), *Al-Waqa'I' al-Misriyah*, 5 Aug. 1937, No. 71, pp. 58-87 (Egypt).
[125] ANDERS HENRIKSEN, *supra* note 104*,* at 92.
[126] *See* discussion *infra* Ch. 5.
[127] DANIELLE IRRELAND-PIPER, *supra* note 99*,* at 17.
[128] International Civil Aviation Organization, *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation* 128, Sep. 23, 1971, 974 U.N.T.S 177 (entered into force Jan. 26, 1973).

the territorial principle. After a long negotiation, it was agreed that a trial would be held in the Netherlands in a court deemed to be a Scottish court. In this way, this conflict between the competing states over jurisdiction was resolved by reaching a compromise solution.

Regarding cybercrime, most national laws assert jurisdiction if the crime is committed by one of the state's nationals. Examples are Article (3) of Egyptian Law,[129] Article (33) of the Nigerian Cybercrime Act of 2015,[130] and Article (27) of Cybercrime Law of Portugal No. 109 for the year of 2009.[131] Also, in the international sphere, Article (22) of the Budapest Convention provides for the nationality principle as a ground for jurisdiction.[132] Finally, the nationality principle is applicable to natural persons as well as to juristic persons. Therefore, the service providers being adhering to the territorial principle, may also be subject to the nationality principle in relation to obligation and wrongful acts.[133]

3. Passive Nationality Principle

The third base for exercising jurisdiction is the passive nationality principle which is based on the nationality of the victim. This ground gives a state the jurisdiction to prosecute and adjudicate a foreigner irrespective of his/her nationality for a crime he/she committed outside its territory against its national(s).[134] Indeed, many countries seek to protect its nationals abroad against serious crimes such as terrorism, human trafficking, and cybercrime by applying their laws on the perpetrators of these crimes committed outside local territories against their nationals.

Historically, the application of this principle has been criticized and objected to for several reasons. First, it is not accepted because the interest of the state to punish the offenders who committed a crime against their nationals abroad was not seen as an

---

[129] Egyptian Anti-Information Technology Crimes Law, *supra* note 77, art. 3.
[130] Cybercrimes (Prohibition, Prevention, Etc.) Act (2015), (Nigeria) [hereinafter Nigerian Law on Cybercrime].
[131] Law No. 109 of 2009 (Law on Cybercrime), 15 Sept. 2009 (Portugal) [hereinafter Portuguese Law on Cybercrime].
[132] Convention on Cybercrime, *Surpa* note 8, at 13.
[133] Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet*, 50 Fed. Comm. L.J. 117, 132 (1997).
[134] MARTIN DIXON, TEXTBOOK ON INTERNATIONAL LAW 152 (6th ed. 2007).

essential one or an extension of the statehood. Second, state' nationals enjoy the protection of the territorial state and the exercise of jurisdiction based on the passive nationality principle means that the territorial state is not able to protect all its inhabitants, including foreign nationals which was not accepted.[135]

Third, this principle creates uncertainty about the acts that are considered legal within a state because a person may be held liable in a foreign state for an act committed against one of its nationals even though this act was not illegal in the state where it occurred. Fourth, the potential offender will not be able to predict which state' laws he may be subjected to as he does not usually know the nationality of victim(s).[136]

Fifth, this principle could cause an extensive tension between the concerned states when the act which is a crime under the law of the state of the victim's nationality is not criminalized under the law of the state where it occurred or the state's law of the perpetrator's nationality. Sixth, the practical effect of the application of the passive personality rule is that a person will have the protection of the law of his/her nationality's state wherever he/she exists. Therefore, all persons who have contacted with him/her are themselves subject to this law.[137]

There are many examples that reflect such opposition to the passive nationality principle. In *the S.S 'Lotus' France v. Turkey,* all of the dissenting judges expressly rejected the application of this principle.[138] Also, in *the Cutting Case Mexico v. USA,*[139] a U.S. citizen has charged with a libel against a Mexican national in the USA. He was arrested during a trip to Mexico upon the application of the passive nationality principle. As a result, the USA Government strongly protested Mexico's exercise of its jurisdiction based on this principle. In addition, the commentary on Article (10) of the Draft Convention on Jurisdiction with Respect to Crime reveals opposition to this principle as a basis for jurisdiction because it is considered to cause controversy without serving any useful objective.[140]

---

[135] LOUIS HENKIN, INTERNATIONAL LAW: POLITICS AND VALUES 239 (1995).
[136] ANDERS HENRIKSEN, *supra* note 104, at 88.
[137] MARTIN DIXON, *supra* note 134*,* at 153.
[138] ALINA KACZOROWSKA-IRELAND, *supra* note 103, at 364.
[139] Ikenga K.E. Oraegbunam, *supra* note 35*,* at 29.
[140] ANDERS HENRIKSEN, *supra* note 104*,* at 87.

Due to the increase in terrorist attacks and other internationally condemned crimes, nowadays, there is less rejection for the passive personality principle as an accepted ground for jurisdiction. In reality, there are several examples that prove the positive tendency for the application of this principle. In *US v. Yunis*, US agents arrested a Lebanese citizen in international water and brought him for prosecution in the USA for alleged involvement in the hijacking of a Jordanian aircraft. In this case, U.S Court based its jurisdiction upon the universality principle and the passive personality principle because there were several American nationals on that flight.[141] Another instance is when U.S authorities relied on this principle in 1985 to prosecute a group of terrorists who had hijacked an Italian cruise ship called the *Achille Lauro* and murdered an American passenger.[142]

In relation to cybercrime, many national laws extend their jurisdiction to cover the cybercrime that is committed against their national(s) outside national territories. For example, Article (3) of Egyptian Law,[143] Article (33) of the Nigerian Cybercrime Act of 1995.[144] Nevertheless, the increased use of this principle results in a situation of concurrent jurisdictions over the same cybercrime that will be discussed later in chapter five.[145]

4. **Protective Principle**

The fourth basis for jurisdiction is the protective principle which is based on the protection of essential interests of a state. Traditionally, it has been recognized that states have a legitimate interest in safeguarding their vital national interests such as national security and economy against certain crimes like espionage, the falsification of official documents, cybercrime, and different forms of transnational organized crimes which are committed abroad by subjecting the offenders of those crimes to their national law. However, the list of the essential interests is not limited and may differ from one state to another .i.e. certain interests may be important for one country whereas not

[141] MALCOLM N. SHAW, *supra* note 98*,* at 498.
[142] ANDERS HENRIKSEN, *supra* note 104*,* at 88.
[143] Egyptian Anti-Information Technology Crimes Law, *supra* note 77, art. 3.
[144] Nigerian Law on Cybercrime, *supra* note 130, art. 33.
[145] *See* discussion *infra* Ch. 5.

being as such for another country.[146] Nevertheless, there is a great uncertainty regarding crimes that are covered by this principle i.e. what crimes are subject to a state's jurisdiction even if committed outside its boundaries by foreigners.[147]

Indeed, the American law has traditionally provided for the extension of jurisdiction over certain offenses when the conduct has been committed abroad as long as the harmful effect or result occurred within the USA' territorial boundaries.[148] For example, in *United States v. Zehe,*[149] it was held that the USA had the jurisdiction over the alleged act of espionage which was committed in Mexico and the German Democratic Republic by an East German citizen against the USA. Such an assertion of jurisdiction was based on the protective principle which allowed the USA to impose its jurisdiction over the act committed abroad either by its own nationals or foreigners which threatened its security.

There are two main arguments in favor of the development of this principle in the international law as an exception to the exclusive jurisdiction of the territorial or nationality state. First, all states have such interests and seek to maintain their power to protect them so that they are ready to give up their power as a territorial state or a state of nationality on a reciprocal basis if another state claims its jurisdiction based on the protective principle. Second, the territorial state and the state of nationality could have no interest in prosecuting such crimes or the ability to do so effectively. Therefore, the effected state has a legitimate interest in prosecuting them otherwise they could go unpunished.[150] Indeed, this principle can achieve a legitimate interest of a state to counter crimes committed by aliens abroad which have an adverse effect on its security and welfare. Therefore, it is regarded as an accepted basis of jurisdiction under the customary international law.[151]

---

[146] Vaughan Lowe & Christopher Staker, *Jurisdiction,* in INTERNATIONAL LAW 342 (MALCOLM D. EVANS, Ed., 3d ed. 2010).
[147] MALCOLM N. SHAW, *supra* note 98, at 499.
[148] Christopher L. Blakesley, *supra* note 105*,* at 1123.
[149] ADEMOLA ABASS, *supra* note 116*,* at 538.
[150] LOUIS HENKIN, *supra* note 135*,* at 238-39.
[151] MARTIN DIXON, *supra* note 134*,* at 150.

There is always the risk that some states may abuse this principle by applying a very broad interpretation of this doctrine by expanding their jurisdiction to protect an unvital interest.[152] There is also a danger that this principle may be used by one state to punish acts committed abroad which are protected as civil freedoms by the state within its territory these acts occurred such as the freedom of press and speech.[153]

In addition, the application of this principle can cause a practical problem if the act committed abroad is a crime under the law of the state against its interest this act was committed but is not illegal under the law of the state where it occurred. Thus, it has been suggested that this principle should not be applied if the act is lawful under the law of the state where it took place in order to avoid unnecessary tension between the concerned states.[154] Furthermore, the extensive utilization of this principle will definitely lead to a conflict of jurisdiction between states which will be discussed later in chapter five.[155]

Regarding cybercrime, many national laws extend their jurisdiction over cybercrime committed abroad when it targets computer systems located within their territories. Examples are Article (3) of Egyptian Law,[156] Article (47) of the Emirati Anti-Information Technology Crimes Law No. 5 for the year of 2012,[157] and Article (2) of the Electronic Information and Transactions Law of Indonesia No. 11 of 2008.[158]

Also, there are several examples that prove the positive tendency for the application of this principle in relation to cybercrime, In the *Ttiben case*,[159] one Australian national posted material on a web site that denied the existence of the Holocaust. He was charged with inciting racial hatred by a German Court that assumed jurisdiction on the basis of

---

[152] ALINA KACZOROWSKA-IRELAND, *supra* note 103*,* at 361.
[153] THOMAS BUERGENTHAL & HAROLD G. MAIER, PUBLIC INTERNATIONAL LAW 172 (2d ed. 1990).
[154] MARTIN DIXON, *supra* note 134*,* at 151-52.
[155] *See* discussion *infra* Ch. 5.
[156] Egyptian Anti-Information Technology Crimes Law, *supra* note 77, art. 3.
[157] (Anti-Information Technology Crimes Law), 13 Aug. 2012 (United Arab Emirates) [hereinafter Emirati Anti-Information Technology Crimes Law].
[158] Law No. 11 of 2008 (Law on Electronic Information and Transaction), 21 Apr. 2008 (Indonesia).
[159] Ray August, *supra* note 102*,* at 541.

the protective principle to protect a legitimate national interest which is a segment of the national population from being defamed.

5. Universality Principle

The fifth and final basis for jurisdiction is the universality principle which is based on the international character of the offense that allows a state's judicial system to prosecute and adjudicate an offender of a *jus cogens* crime such as piracy and genocide even though there is no connection between this state and the committed crime.[160] That is because these crimes are so serious and disruptive to the international community that any state can exercise its jurisdiction over them irrespective of where they have been committed or the nationality of the offenders or victims.[161]

Therefore, the application of universal jurisdiction is the most efficient way to counter and prevent international crimes by raising the possibility of prosecution and punishment of offenders.[162] To such effect, many states such as Belgium and Spain have issued national legislation which explicitly establishes their universal jurisdiction over certain crimes.[163]

Historically, the notion of universal jurisdiction was developed to counter the crime of piracy because the pirates commonly roamed the high seas outside the territorial jurisdiction of any state which is not regulated by the national laws. Therefore, the universal jurisdiction was created to fulfil the jurisdictional vacuum by allowing all states to prosecute any pirate they could apprehend and the international customary law confirmed the states' right to assert their jurisdiction over this crime.[164] Then, the application of universal jurisdiction was extended to cover other *jus cogens* crimes to

---

[160] Kenneth C. Randall, *Universal Jurisdiction under International Law*, 66 Tex. L. Rev. 785, 788 (1988); *see also* Gerhard Erasmus & Gerhard Kemp, *Application of International Criminal Law before Domestic Courts in the Light of Recent Developments in International and Constitutional Law*, The, 27 S. Afr. Y.B. Int'l L. 64, 65-66 (2002).
[161] ANDERS HENRIKSEN, *supra* note 104, at 90.
[162] M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice*, 42 Va. J. Int'l L. 81, 153 (2001).
[163] REBECCA M.M. WALLACE & OLGA MARTIN-ORTEGA, *supra* note 113, at 131.
[164] ANDERS HENRIKSEN, *supra* note 104, at 90.

include slavery, crimes against humanity, war crimes, genocide, torture, and apartheid.[165]

However, it is strongly recommended that the application of universal jurisdiction must be controlled. Otherwise, it will be destructive to the international legal processes and would produce continuous conflicts of jurisdiction between states that may threaten the world order and subject individuals to human rights violations, politically motivated harassment, and abuses of judicial processes. Therefore, it is inevitable to develop guidelines regulating the resort by states and international adjudicating bodies to the application of this principle. Then, such guidelines, after acquiring the required international consensus, should be reflected in an international convention.[166]

In reality, one of the most important cases that involves the application of this principle is *Democratic of the Congo. V. Belgium*.[167] When Belgium issued an international arrest warrant against the acting Congolese Minister of Foreign Affairs due to his grave violation of international humanitarian law and based the assertion of its jurisdiction on the universal principle as there was no connection between Belgium and this crime.

In relation to cybercrime, it is argued that the universal jurisdiction which allows one state to prosecute certain crimes even in the absence of any connection should be extended to cover cybercrime. Thus, such application can solve the inherent jurisdictional problems associated with the commission of cybercrime to include where the crime occurred, who will investigate it, and where the crime will be prosecuted. Also, this principle is suited to the transnational nature of cybercrime as the offender can commit a cybercrime which causes damage to victims in more than one country. Even though, such opinion recognizes that it is still unclear as to what extent the universal jurisdiction should apply to cybercrime.[168] On the contrary, it is contended that cybercrime can not be subjected to the universal jurisdiction unless it causes a vital

[165] M. Cherif Bassiouni, *supra* note 162, at 108.
[166] M. Cherif Bassiouni, *supra* note 162, at 154-55.
[167] MARTIN DIXON, *supra* note 134, at 148.
[168] Frances P Bernat & Nicholas Godlove, *Understanding 21 st century cybercrime for the 'common' victim,* 89 CRIM. JUST. MATTERS, 4, 4 (2012).

violation of human rights that constitutes one of the heinous international crimes such as crime against humanity.[169]

Similarly, in relation to a cyberterrorism crime that can be defined as the use of computer technology to commit a terrorist act,[170] there is a view that universal jurisdiction has a broad reach as it gives a state authority the power to prosecute certain international crimes even though no connection exists. Therefore, this principle is the most effective method for deterring cyberterrorism crimes by defeating the inherent practical challenges resulted from those terrorists committing their crimes in cyberspace with the aim of establishing their accountability in order to enhance international peace and justice.[171]

In fact, there are several arguments in favor of such application. First, cyberterrorism crime imposes several practical difficulties for law enforcement authorities in the investigation and prosecution process especially the difficulty in knowing the identity of cyberterrorist or the location of computer used to launch the attack. Hence, such obstacles make it difficult to apply territorial jurisdiction. Therefore, the application of universal jurisdiction that does not require any connection between the state and the crime can overcome these challenges so that it is the most effective mean to deter a cyberterrorist crime.[172] Second, the heinous nature of this crime is equivalent to the core international crimes like genocide and crimes against humanity which are subject to universal jurisdiction.[173] Thus, cyberterrorism as well should subject to the universal jurisdiction.

Third, the customary international law recognizes terrorism and subsequently cyberterrorism as an international crime that could subject to universal jurisdiction. That is proved by state practice and *opinio juris* as states believe that terrorism is a heinous

---

[169] Fausto Pocar, *New Challenges for International Rules Against Cyber-crime*, 10 EUR. J. ON CRIM. POL'Y AND RES., 27, 37 (2004).
[170] SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE 37 (2009).
[171] Kelly A. Gable*, supra* note 45, at 105.
[172] *Id* at 103-04.
[173] Pardis Moslemzadeh Tehrani & Nazura Abdul Manap & Hossein Taji, *Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime,* 29 COMPUTER L. & SECURITY REP 207, 209 (2013).

crime against humanity and the international order which is reflected in the conclusion of nineteen international legal instruments to prevent terrorism acts.[174] As well, there are several resolutions issued from the United Nation Security Council and General Assembly that condemn terrorist acts especially those committed through or by the Internet and states are called upon to enhance the international cooperation in this respect. As a result, states and international organizations are actively working to implement these resolutions which confirms the existence of both *opinio juris* and state practice.[175]

I agree with the opinion adopted by several experts who confirm that terrorism is a transnational but not an international crime for several reasons. First, all the international instruments in relation to terrorism do not provide for universal jurisdiction over any form of terrorist act but only require states to criminalize certain conducts, establish extraterritorial jurisdiction over them, and cooperate with each other in the prosecution and extradition of the offenders. Second, countries refused the proposal to include terrorism as a separate crime under the Rome Statute which established and governs the International Criminal Court. Third, there is no universally accepted definition of terrorism and all efforts to establish such a definition have been failed.[176] For all of these reasons, I contend that terrorism is not one of the international crimes.

However, many authors contend that there is a universal definition of terrorism as an international crime in the time of peace which has evolved via international customary law. Regardless, they admit that there is still controversy over whether the definition may also be applied in time of armed conflict due to the disagreement in relation to whether acts performed by freedom fighters' in wars of national liberation may (or should) constitute an exception and not be considered as a terrorism crime.[177]

---

[174] UNITED NATION Office of Countering Terrorism, International Legal Instruments, https://www.un.org/en/counterterrorism/legal-instruments.shtml.
[175] Kelly A. Gable, *supra* note 45, at 106-07. *See also* Christian Much, *International Criminal Court (ICC) and Terrorism as an International Crime*, The , 14 MICH. ST. J. INT'L L. 121, 125 (2006).
[176] Jonathan Hafetz, *Terrorism as an International Crime: Mediating between Justice and Legality*, 109 AM. SOC'Y INT'L L. PROC. 158, 159 (2015).
[177] Antonio Cassese, *The Multifaceted Criminal Notion of Terrorism in International Law*, 4 J. INT'L CRIM. JUST.933, 933 (2006).

B. The Expansive Jurisdiction Approach over Cybercrime

After elaborating the different bases for exercising the criminal jurisdiction by the states, this section shows how law reforms have expanded territorial jurisdiction and established extraterritorial jurisdiction as a policy response to the cybercrime phenomenon and its transnational dimension.[178] Indeed, the drafters of several national laws and international or regional cybercrime instruments adopt a broad approach in relation to the jurisdiction over this crime. As a result, jurisdiction over cybercrime can be established based on several bases including territorial, active nationality, passive nationality, and protective principles.

At the international level, one of the main objectives of the Convention against Transnational Organized Crime and other cybercrime' conventions is to make sure that there is no safe haven for the criminal and ensure that every illegal action will be adjudicated. Therefore, most of these conventions provide for an expansive approach in relation to the jurisdiction.

For example, according to Article (30) of the Arab Convention,[179] state party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in this Convention, if the offence is committed, partly or totally, or was realized:

- In the territory of the state party.
- On board a ship raising the flag of the State Party.
- On board a plane registered under the law of the State Party.
- By a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State.
- If the offence affects an overriding interest of the State.

Another instance, according to Article (22) of the Budapest Convention,[180] each state party shall adopt such legislative and other measures as may be necessary to establish

[178] IAN WALDEN, COMPUTER CRIMES AND DIGITAL INVESTIGATIONS 306 (2007).
[179] Arab Convention on Combating Information Technology Offenses, *supra* note 9, at 14.
[180] Convention on Cybercrime, *supra* note 8, at 13.

jurisdiction over any offence set forth in this Convention, when the offence is committed:

- In its territory.
- On board a ship flying the flag of that Party.
- On board an aircraft registered under the laws of that Party.
- By one of its nationals if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

Likewise, at the national level, several countries have responded to the challenge of transnational cybercrime by expanding their jurisdiction over this crime.[181] For example, Article (3) of the Egyptian Law adopts the territorial, active nationality, passive nationality, and protective principles as bases to establish jurisdiction over any cybercrime.[182] In fact, the Egyptian legislator adopts the same approach in relation to crimes that could be associated with a transnational dimension such as Article (16) of Combating Human Trafficking Law,[183]Article (20) of Combating Illegal Migration and Smuggling of Migrants Law,[184]and Article (4) of Anti-Terrorism Law.[185] Also, the Article (47) of the Emirati Anti-Information Technology Crimes Law No. 5 for the year of 2012,[186]and the Article (27) of the Cybercrime Law of Portugal No. 109 for the year of 2009,[187]adopt the same grounds as Egyptian law in terms of jurisdictional bases over cybercrime.

C. Conflict of Jurisdiction in Cybercrime

In fact, this previously mentioned expansive approach to exercising jurisdiction over cybercrime can lead to the situation whereby two or more countries assert their jurisdiction based on the application of either similar or different jurisdictional claims

[181] Peter Grabosky*, supra* note 31, at 151.
[182] Egyptian Anti-Information Technology Crimes Law, *supra* note 77, art. 3.
[183] Law No. 64 of 2010 (Law on Combating Human Trafficking), *Al-Jarida Al-Rasmiyya*, 9 May. 2010, No. 18 bis, pp. 5-14 (Egypt).
[184] Law No. 82 of 2016 (Law on Combating Illegal Migration and Smuggling of Migrants), *Al-Jarida Al-Rasmiyya*, 7 Nov. 2016, No. 44 bis [a], pp. 2-15 (Egypt).
[185] Law No. 94 of 2015 (Anti-Terrorism Law), *Al-Jarida Al-Rasmiyya*, 15 Aug. 2015, No. 33 bis, pp. 3-26 (Egypt).
[186] Emirati Anti-Information Technology Crimes Law, *surpa* note 157, art. 47.
[187] Portuguese Law on Cybercrime, *supra* note 131, art. 27.

over the same cybercrime. Then, they initiate parallel proceedings for the same facts that lead to a positive jurisdictional conflict between them.[188]

Unlike the positive conflict of jurisdiction, the negative conflict may occur when no country claims its jurisdiction over a certain cybercrime. In reality, this situation is very rare due to the increased number of international and regional cybercrime agreements which oblige the state members to criminalize different forms of cybercrime.[189] Subsequently, most of the countries around the world have now a legislation against cybercrime.[190]

One example of positive conflict of jurisdiction over the same cybercrime is if one person in the United Arab Emirates spread a serious virus on the Internet which caused massive harm to many Egyptian and Nigerian nationals in the United Arab Emirates and governmental institutions in several countries, including Singapore and Portugal. Each country would claim its jurisdiction to investigate, prosecute and adjudicate this crime according to the jurisdiction clause in its domestic law. Indeed, the United Arab Emirates has a jurisdiction clause based on the territorial principle, whereas, Egypt and Nigeria have jurisdiction based on the passive nationality principle. One the other hand, Singapore and Portugal have a jurisdiction according to the protective principle. Therefore, there will be a positive conflict of jurisdiction between several states over the same cybercrime and the critical question here is how to resolve this conflict.

Indeed, the drafters of several international conventions include a broad jurisdiction clause aiming at denying safe havens for criminals while recognizing the possibility of jurisdiction clash as a result of such an expansive clause. Nevertheless, they believe that this situation is rare and can be resolved through the negotiation between the concerned states in order to determine the best jurisdiction for the successful prosecution and adjudication of a particular case.[191]

---

[188] IAN WALDEN, *supra* note 178, at 306.
[189] Henrik W.K. Kaspersen, *Cybercrime and internet jurisdiction* 1, 6 (2009), https://rm.coe.int/16803042b7.
[190] Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. High Tech. L. 1, 40 (2004).
[191] Roger S. Clark, *The United Nations Convention against Transnational Organized Crime*, 50 Wayne L. Rev. 161, 181 (2004).

However, this conflict in reality raises many practical issues including the impediment of effective and rapid international cooperation between the competing states. This is particularly true in relation to extradition and mutual legal assistance requests as each concerned state will claim its jurisdiction over the crime and reject the jurisdiction of other states. Thus, a state will refuse to provide its assistance either through mutual legal assistance or extradition.[192] Moreover, the issue is even more sophisticated if the perpetrator exists in a country with no jurisdictional claim and all the concerned states ask for the extradition or seek mutual legal assistance from this country. For example, in the pre-mentioned hypothetical case, if the accused person fled the United Arab Emirates to Kuwait, a very critical situation regarding to which country the accused person should be extradited to would result.

Also, this conflict could lead to the violation of the *non bis in idem* principle that does not allow an alleged perpetrator to be prosecuted and punished more than one time for the same criminal act as the duplication of procedures and penalties involves the unacceptable repetition of the exercise of the *ius puniendi.*[193] Indeed, the principle of *ne bis in idem* is a basic principle of the European and international criminal justice as well as national criminal law. For example, Article (14/7) of International Covenant on Civil and Political Rights (ICCPR) states that "No one shall be liable to be tried or punished again for an offense for which he has already been finally convicted or acquitted in accordance with the law and penal procedure of each country".[194] Furthermore, such conflict may result in inconvenience for witnesses, the duplication of efforts, or competition between law enforcement officials of the states concerned which should be avoided.[195]

Therefore, it is a must to find a solution to such situations of concurrent jurisdictional claims by deciding which country should be given the exclusive right to prosecute and adjudicate the involved cybercrime. It is not an easy task to reach such an outcome for

[192] Henrik W.K. Kaspersen, *supra* note 189, at 6.
[193] Wolfgang Schomburg, *Criminal matters: transnational ne bis in idem in Europe—conflict of jurisdictions—transfer of proceedings*, 13 ERA F. 311, 312 (2012).
[194] International Covenant on Civil and Political Rights 177, Dec. 19, 1966, 1057 U.N.T.S 407 (entered into force Mar. 23, 1976).
[195] Explanatory Report to the Convention on Cybercrime, *supra* note 73, at 41.

several reasons. Firstly, it is recognized that each state has the sovereign power to impose its jurisdiction over conducts occurring within its territory and, beyond it, such other conducts which affect its legitimate interests.[196] Secondly, the international law recognizes the equality between all states in the world and does not give any of them a hierarchical authority over the others.[197] Thirdly, the general international law has not established a system of priority among different jurisdictional bases.[198] Fourthly, the principles of jurisdiction under the international law do not resolve such dilemma of concurrent jurisdictional claims.[199]

Indeed, some scholars suggest a specific hierarchy among the different jurisdictional theories in the situation of positive conflict of jurisdiction by giving the first priority to the territorial principle over other jurisdictional claims. Then, the universality principle, the protective theory, the active nationality principle, and finally, the passive nationality principle. Nevertheless, they confirm that there is still no clear rule which establishes such a hierarchy in the international law in the case of concurrent jurisdictional claims.[200]

In addition, at the national level, countries have confirmed that, during the information gathering stage for the United Nation Office on Drugs and Crime's Comprehensive Study, they did not have specific legislation intended to resolve conflict of jurisdiction in cybercrime.[201]

In sum, this chapter has represented in detail the different bases for jurisdiction and their value in the contemporary international law and how the main characteristics of cybercrime have encouraged the establishment of extraterritorial jurisdiction over this crime that may result in the occurrence of a positive conflict of jurisdiction. However, there is no conclusive agreement on one effective solution to positive jurisdiction's conflict among states in cybercrimes cases either in the international instruments or in

[196] M. Cherif Bassiouni, *Theories of Jurisdiction and Their Application in Extradition Law and Practice*, 5 Cal. W. Int'l L.J. 1, 2 (1974).
[197] HANS KELSEN, PRINCIPLES OF INTERNATIONAL LAW 155 (2003).
[198] Roger S. Clark, *supra* note 191, at 181; *see also* ANDERS HENRIKSEN, *supra* note 104, at 92.
[199] DANIELLE IRRELAND-PIPER, *supra* note 99, at 2.
[200] M. Cherif Bassiouni, *supra* note 196, at 59-60.
[201] Comprehensive Study on Cybercrime, *supra* note 2, at 195.

the literature. The next chapter demonstrates the different opinions offered for solving the issue of competing jurisdictional claims over the same cybercrime. It concludes with suggestion for reaching a decision which can solve such a conflict.

V. Moving Forward to Overcome Conflict of Jurisdiction in Cybercrime

It a must to set up an effective mechanism in order to resolve this conflict of jurisdiction arises in relation to cybercrime. This chapter shows in detail the different approaches to managing this conflict in order to compare the advantages and disadvantages of each view. In fact, these approaches include the opinion which favors the negotiation between the concerned states aiming at centralizing the criminal proceeding in one single country; the view that prefers the establishment of an obvious, concrete, and binding rule which decides the priority among the competing jurisdictional claims; and the opinion which supports the development of a guideline which includes certain factors to be evaluated in order to reach a decision settling this conflict. This chapter then proposes a solution by providing for certain factors with different weight to be assessed and evaluated in order to decide the best jurisdiction among the concurrent ones for being granted the exclusive competence over the cybercrime taking into consideration the characteristics of cybercrime and the facts of each single case.

A. Evaluating Different Approaches Regarding the Positive Conflict of Jurisdiction

In general, regarding civil and commercial matters, the international community especially the European Union has established an almost complete set of regulations on jurisdiction that provides the different parties with the ability to know in advance whether a specific court has or does not have the authority to decide the case brought before it with very little space for uncertainty and incoherence. Conversely, in criminal issues there is no set of agreed rules to decide which country should be given the jurisdiction over a crime in situation of a positive conflict even within the United Nations or European Union legal systems.[202]

Moving to cybercrime, the same dilemma exists when there is a conflict over competence between two or more countries. Looking at the literature, it appears that there is an obvious recognition of the serious consequences in the case of concurrent jurisdictional claims which may affect negatively international cooperation in the fight against cybercrime and cause the violation of the fundamental principle of *ne bis in idem*. Such a conflict should be avoided in the interest of justice by choosing the best

[202] Ignazio Patrone, *Conflicts of jurisdiction and judicial cooperation instruments: Eurojust's role*, 14 ERA F. 215, 216 (2013).

jurisdiction in a transparent and objective way in order to improve the judicial cooperation in criminal matters.[203] In addition, it is a must to reach a solution to such a conflict at the very beginning of the criminal proceedings because it is clearly inadequate when a judge decides that he has no jurisdiction relating to a certain crime after a long and complicated investigation.[204]

Nevertheless, there is no conclusive agreement on one agreed solution to such a positive conflict of jurisdiction. Looking at the literature, there are three different ways to deal with such a dilemma. The first opinion confirms that since the general international law has not established a system of priority among different jurisdictional theories. Therefore, in the case of competing jurisdictional claims between two or more states the best solution is conducting a fruitful negotiation between the concerned states in order to decide the best state jurisdiction for a successful prosecution and adjudication of the involved case.[205]

In reality, such a position is adopted in many international instruments. For example, Article (15/5) of the United Nations Convention Against Transnational Organized Crime provides that "if a State Party exercising its jurisdiction under paragraph 1 or 2 of this Article has been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions."[206] In such way, this Article encourages the negotiation and coordination between states parties in the case of positive conflict of jurisdiction.

The same position is adopted in Article (22/5) of the Budapest Convention which provides that "when more than one Party claims jurisdiction over an alleged offense established in accordance with this Convention, the Parties involved shall, where

[203] Aghenitei Mihaela & Flamanzeanu Ion, *Analysis Conflicts of Jurisdiction in Criminal Proceedings to the European Union Legal Framework*, 2010 AGORA Int'l J. Jurid. Sci. [cxlv], [cxlix] (2010).
[204] Ignazio Patrone, *supra* note 202, at 217.
[205] Roger S. Clark, *supra* note 191, at 181.
[206] United Nations Convention against Transnational Organized Crime, *supra* note 17, at 16.

appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[207]

Indeed, the proponents of such a view allege that such negotiation has many advantages as it allows the concerned states to choose a single venue for legal proceedings or to authorize one state to prosecute certain perpetrators and another state to prosecute another group of alleged offenders if such a solution is the most appropriate one for the interest of the legal proceedings against the committed crime.[208] In addition, I argue that such negotiation may effectively encourage the implementation of the different forms of international cooperation especially the establishment of joint investigation team between the authorities of the concerned states which can deal effectively with a cybercrime that has a transnational nature in terms of the collection of evidence and apprehension of the offenders.

Furthermore, supporters to this opinion confirm that the agreement resulting from the consultation and negotiation between the involved states can be legally implemented by resorting to the mechanism of transferring of criminal proceedings commenced in one country to be conducted in another state.[209] For example, according to Article (3) of the European Convention on the Transfer of Proceedings in Criminal Matters "Any Contracting State having competence under its own law to prosecute an offense may, for the purposes of applying this Convention, waive or desist from proceedings against a suspected person who is being or will be prosecuted for the same offense by another Contracting State."[210]

In contrast, many authors argue that there are many disadvantages linked to this opinion that prefers the negotiation as a mean to settle this conflict of jurisdiction. First, it merely encourages the concerned states to solve the dilemma of dispute over jurisdiction

---

[207] Convention on Cybercrime, *surpa* note 8, at 14.
[208] Armando A. Cottim, *supra* note 112, at 67; *see also* Explanatory Report to the Convention on Cybercrime, *supra* note 73, at 41.
[209] IAN WALDEN, *supra* note 178, at 307; *see also* United Nation Manual on the prevention and control of computer- related crime, 25 (2001), http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf.
[210] Council of Europe, European Convention on the Transfer of Proceedings in Criminal Matters 2, May. 15, 1972, E.T.S No. 073 (entered into force Mar. 30, 1978).

through consultation and mutual agreement which is rare in practice without providing the states with concrete guidelines setting up a mechanism for prioritizing jurisdictional claims. This mechanism establishes certain factors to be considered in reaching a decision solving such conflict. Second, as long as the conflict of states' jurisdictions becomes more common, negotiation is likely to be less satisfactory because it does not provide the involved states with the ability to predict the outcome and it is time-consuming.[211]

Third, according to the Explanatory Report of the Budapest Convention, consultation is not obligatory. Thus, if a state believes that consultation may impair or delay its investigation or proceedings, it may refuse to conduct any consultation with the other state(s).[212] The Budapest Convention is criticized because it does not establish an effective mean for resolving the possible positive conflict of jurisdiction either by determining certain and clear guidelines or setting up a mechanism for prioritizing jurisdictional claims.[213] For all of these reasons, the only dependence on the negotiation is not suitable to settle this dilemma.

Unlike the first approach, the second opinion contends that the most effective solution to such conflict is to establish an obvious, concrete, and binding rule which determines the priority among the competing national jurisdictional theories.[214] Such a position is followed by Article (30/3) of the League of Arab States Convention, which provides for an explicit order of priority for competing jurisdictional claims as follows: (i) states whose security or interests have been disrupted by the offense; (ii) states in whose territory the offense was committed; and (iii) the state of nationality of the offender. If no balance can be found according to this order, then priority is accorded to the first requesting state.[215]

---

[211] Susan W. Brenner, *supra* note 37, at 197.
[212] Explanatory Report to the Convention on Cybercrime, *supra* note 73, at 41.
[213] Susan W. Brenner & Bert-Jaap Koops, *supra* note 190, at 42.
[214] Shannon L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, 2 J. High Tech. L. 101, 118 (2003); *see also* M. Cherif Bassiouni, *supra* note 196, at 61.
[215] Arab Convention on Combating Information Technology Offenses*, supra* note 9, at 15.

Also, Article (10) of EU Council Framework Decision 2005/222/JHA on attacks against information systems[216] allows each member state to establish its jurisdiction if the offence has been committed in whole or in part within its territory, by one of its nationals, or for the benefit of a legal person that has its head office in its territory, or against an information system on its territory whether or not the offender committed the crime when physically present on its territory. In the case of concurrent jurisdiction claims, the concerned states must cooperate to centralize the proceedings in one state. Also, they may recourse to a body or mechanism within the EU to facilitate their judicial cooperation and sequential account may be given first to the state where the crime has been committed or against an information system in its territory; then, the state of the perpetrator nationality; after that, the state in which the perpetrator has been found.

In fact, this opinion is criticized because it is not an easy task to establish a hierarchy among different jurisdictional bases. Furthermore, such a rule is very rigid which cannot accommodate with the circumstances and particularities of each case. The determination on which jurisdiction is the best venue to investigate and prosecute should be based on the facts and circumstances of every single case.[217] Thus, I agree that this approach is not adequate for deciding in advance the best jurisdiction for the trial and is not suitable to the uniqueness of a particular case of cybercrime.

The third approach argues that there should be a guideline which determines certain factors to be considered in order to reach a decision solving such positive conflict of jurisdiction between countries. In addition, the supporters of such opinion allege that these factors are not necessary to be given equal weight, are not intended to be exhaustive, and should serve as elements that structure the general assessment of whether it is "reasonable" to assign the jurisdiction to Country A, Country B or Country C in a particular case. In addition, the proponents of such view contend that these factors will not only help in giving a solution to the dilemma, but also providing the states with the ability to predict the outcome if the dispute over jurisdiction exists aiming at preventing the conflict at the very beginning or before its occurrence.[218]

---

[216] EU Council Framework Decision 2005/222/JHA, art. 10/4, 2005 O.J. (L 69/67).
[217] United Nation Manual on the prevention and control of computer- related crime, *supra* note 209, at 26; *see also* Susan W. Brenner, *supra* note 37, at 198.
[218] Susan W. Brenner, *supra* note 37*, at* 197-98.

In reality, The European Union's Judicial Cooperation Unit (Eurojust) adopts such an opinion as according to Article (7) of the Eurojust decision 2009/426/JHA on the strengthening of Eurojust which amends decision 2002/187/JHA that setting up Eurojust, where two or more national members cannot agree on how to resolve a case of conflict of jurisdiction as regards the undertaking of investigations or prosecution, the Eurojust shall be asked to issue a written non-binding opinion on the case to the member states concerned.[219]

To such effect, 2016 revised Eurojust guidelines for deciding which jurisdiction should prosecute is the most important attempt to organize the issue of concurrent jurisdictional claims in Europe.[220] That is because it provides for the relevant factors that should be considered when issuing the decision on which jurisdiction should prosecute. These factors are territoriality, location of accused person(s), the availability and admissibility of evidence, obtaining evidence from witnesses, experts and victims, protection of witnesses, interests of victims, stage of proceedings, length of proceedings, legal requirements, sentencing powers, proceeds of crime, costs and resources. However, the priority and weight given to each one of these factors are different according to the merits of each case.

B. Factors to be Considered in Solving the Positive Conflict of Jurisdiction

In my opinion, taking into consideration the advantages and disadvantages of the three possible solutions to the dilemma of competing jurisdictional claims between states, I argue that the most effective solution is through the determination of certain factors to be considered and evaluated to decide the best jurisdiction which will take the exclusive competence over the cybercrime according to the facts and merits of each single case and taking into account the transnational nature and other characteristics that distinguish cybercrime from traditional crimes.

---

[219] EU Council Framework Decision 2009/426/JHA, art. 7/2, 2009 O.J. (L 138/14).

[220] GUIDELINES FOR DECIDING 'WHICH JURISDICTION SHOULD PROSECUTE?' 1, 2-4 (Revised 2013), http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Guidelines%20for%20deciding%20which%20jurisdiction%20should%20prosecute%20(2016)/2016_Jurisdiction-Guidelines_EN.pdf.

Indeed, these factors can be utilized by the concerned states in the negotiation process or can be applied by an international body established according to an international instrument with an obligatory mandate to issue a binding decision in the case of conflict between states over competence in cybercrime. One example for such international body is the Eurojust which can issue, upon the request of the concerned states, a written non-binding opinion to solve a conflict over jurisdiction between those states. In reality, the main advantage of this solution is the flexibility to cope with the features of each case.

In addition, these factors should be exhaustive to allow the involved states to predict in advance to whom the jurisdiction should be granted if the dispute arises which shall surely assist in preventing the conflict at the very beginning or before its occurrence. Furthermore, these factors should not be given equal weight as some factors are more relevant than others in the light of transnational nature and other particularities that feature cybercrime. In the end, the decision in this regard will be taken on the basis of an aggregate balance of all these factors i.e. the jurisdiction will be granted to the state which can fulfill many of these factors more than others.

Undoubtedly, the critical question here is how to determine such factors – essentially - what are the criteria that should be taken into consideration for determining these factors. In my opinion, the more effective way is by considering the interests of the different stakeholders in relation to cybercrime that includes like any other crimes, the involved state(s), victim(s), and offender(s). Since it is accepted internationally that a state can impose its jurisdiction in relation to cybercrime based on the territorial, active personality, passive personality, and protective principles. Therefore, these proposed factors should reflect the interest of all the concerned state(s) that can assert their jurisdiction over cybercrime based on any of the previous grounds.

Thus, these suggested factors should include the interest of victim(s), the interest of perpetrator(s), the interest of the state where the crime was committed, the interest of the state of offender's nationality, the interest of the state of victim's nationality, the interest of the state whose one of its vital interests has been affected by the crime. In addition, these factors should contain the interest of criminal proceedings as it is essential to benefit all stakeholders.

1. Interest of the Victim(s)

The first factor to be evaluated is the interest of victim(s) of cybercrime. In most cases, cybercrime involves a transnational dimension because the interconnected nature of the global networks permits the offender in one state to easily commit a cybercrime which affects several victims in many countries without leaving his/her own place.[221] No doubt, such victims have a justified expectation that the state which will be granted the jurisdiction over the cybercrime will conduct the investigation and prosecution extensively and efficiently in a manner that will ensure the conviction of the criminal(s) and give them the opportunity to seek remedies and compensation. Also, they prefer the jurisdiction that can provide them with an effective program for the protection against any revengeful act by the perpetrator(s). Thus, the interest of the cybercrime' victims should be considered as an important factor in determining the best state to prosecute solely a cybercrime subject to the jurisdiction of many countries.

2. Interest of the Perpetrator(s)

Besides the interest of the victim(s), the offender(s)'s interest should be considered as a relevant factor when issuing the decision in favor of one of the competing states over the jurisdiction in relation to the same cybercrime due to the following reasons. First, the perpetrator has an internationally well-recognized right to a fair trial which starts with the investigation process and extends to the final judgement. It includes the following rights:

- The right to equality and equal treatment by the law i.e. the principle of non-discrimination "art (26) of the International Covenant on Civil and Political Rights (International Covenant),[222] and art (24) of the American Convention on Human Rights (American Convention)".[223]
- The right to be presumed innocent until proved guilty throughout the period of criminal investigations and trial proceedings, up to the end of the final appeal "art (14/2) of the International Covenant,[224] and art (6/2) of the

[221] See discussion *supra* note 19.
[222] International Covenant on Civil and Political Rights, *supra* note 194, at 179.
[223] Organization of American States, American Convention on Human Rights 151, Nov. 22, 1969, 1144 U.N.T.S. 123 (entered into force July. 18, 1978).
[224] International Covenant on Civil and Political Rights, *supra* note 194, at 176.

European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention)".[225]

- The right to respect his/her privacy, family, home and correspondence "art (17) of the International Covenant,[226] art (11) of the American Convention,[227] and art (8) of the European Convention".[228]
- The right to be informed promptly and in detail in a language which he understands of the nature and cause of the charge against him, to have adequate time and facilities for the preparation of the defense and to communicate with counsel of his/her own choosing, to have prompt legal assistance upon arrest and detention in order to guarantee the right to an efficient defense and protect the physical and mental integrity deprived of his/her liberty, to have the free assistance of an interpreter if he/she cannot understand or speak the language used in court, and to call or examine witnesses "art (14/3 a,b,d,e,f) of the International Covenant[229] and art (6/3 a,b,c,d,e) of the European Convention".[230]
- The right not to be compelled to testify against himself or to confess guilt or to remain silent "art (14/3 g) of the International Covenant[231] and art (8/2 g) of the American Convention".[232]
- The right to freedom from torture, cruel or inhuman treatment or punishment "art (7) of the International Covenant,[233] and art (5/2) of the American Convention".[234]
- The right to be tried by an independent and impartial tribunal and to have a fair and public hearing and judgement. As well as, to equality of arms and adversarial proceedings "art (14/1) of the International Covenant).[235]

---

[225] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms 3, Nov. 4, 1950, E.T.S No. 005 (entered into force Sept. 3, 1953).
[226] International Covenant on Civil and Political Rights, *supra* note 194, at 177.
[227] American Convention on Human Rights, *supra* note 223, at 148.
[228] Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 225, at 4.
[229] International Covenant on Civil and Political Rights, *supra* note 194, at 177.
[230] Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 225, at 3.
[231] International Covenant on Civil and Political Rights, *supra* note 194, at 177.
[232] American Convention on Human Rights, *supra* note 223, at 148.
[233] International Covenant on Civil and Political Rights, *supra* note 194, at 175.
[234] American Convention on Human Rights, *supra* note 223, at 146.
[235] International Covenant on Civil and Political Rights, *supra* note 194, at 176.

- The right not to held guilty on account of any act or omission that did not constitute a criminal offence at the time it was committed "Art (15/1) of the International Covenant".[236]
- The right not to be tried or punished again for an offence for which he has already been finally convicted or acquitted in accordance with the law and penal procedure of each country "Art (14/7) of the International Covenant[237] and Art (8/4) of the American Convention".[238]
- The right to appeal the judgement "Art (14/5) of the International Covenant".[239]

Second, the offender may have a legitimate interest in refusing the removal from the place where he lives and works to be prosecuted in another state where he does not know the local legal system or langue or the possible punishments may be much greater. In addition, he may possibly not be able to work during the period of the investigation, prosecution, and adjudication processes which will impose a further financial burden. Moreover, in the case of conviction, the defendant still has the right to communicate with his/her family on a regular basis and to receive the rehabilitation and integration programs in his/her own society as well. Furthermore, he must be secured against any act of revenge from the victims in a foreign country that he may be extradited to. Therefore, the offender can raise many arguments against his extradition to another country even if the required conditions according to the applicable treaty exist.[240]

In fact, all of these issues should be considered when assessing the interest of the perpetrator(s) as a relevant factor to be evaluated in determining the best state given jurisdiction over the cybercrime in the case of positive jurisdiction conflict with others.

3. Interest of the State of the Territorial Jurisdiction

The third factor to be assessed is the interest of the state of the territorial jurisdiction. This ground for jurisdiction can be defined as the power of a state to apply its laws over

---

[236] *Id* at 177.
[237] *Id* at 177.
[238] American Convention on Human Rights, *supra* note 223, at 148.
[239] International Covenant on Civil and Political Rights, *supra* note 194, at 177.
[240] Kate Brookson-Morris, *I. Conflicts of Criminal Jurisdiction*, 56 Int'l & Comp. L.Q. 659, 659 (2007).

the crimes that are committed in whole or in part in its territory. Traditionally, the territorial principle has been considered as the most fundamental and well-accepted method of exercising jurisdiction because the place of commission is the best venue to collect the evidence. Therefore, it could be the most convenient venue for the trial.[241]

In fact, many authors still confirm the primacy of territorial principle in relation to jurisdiction over cybercrime because it is usually initiated by an offender who exists in a specific territory of one state.[242] In addition, national laws and the international or regional cybercrime instruments usually provide for the territorial principle as a base for acquiring jurisdiction over the illegal act committed in whole or part in the national territory, on board a ship raising the national flag or on board a plane registered under the national law.[243]

On the contrary, I agree with the opinion that the jurisdiction based on territorial principle has less importance over cybercrime than traditional crimes for several reasons. First, this crime is committed in cyberspace which is an amorphous space that does not occupy a set physical or geographic location i.e. it is an electronic place in which individuals, governments, corporations, and other entities can exist within and beyond the borders of the nation states.[244] Thus, cyberspace has no territorial based boundaries as data can be transported from one physical location to any other location without any substantial delay or physical barriers that might otherwise keep geographically remote places and people separate from each other. Therefore, this architecture of cyberspace undermines the claim that cyberspace should naturally be governed by territoriality defined rules.[245]

Second, it is difficult to pinpoint where the cybercrime actually took place as the criminal usually uses technological tools to make the crime seems to come from elsewhere and he/she may conceal his/her location by looping a large number of

---

[241] See discussion *supra* notes 102, 103.
[242] Henrik W.K. Kaspersen, *supra* note 189*, at* 21; *see also* Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism,* 5 Ind. J. Global Legal Stud. 561, 568 (1998).
[243] Comprehensive Study on Cybercrime, *supra* note 2, at 191-92.
[244] Gerogios I. Zeros, *State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction,* 15 Int'l J.L. & Info. Tech. 1, 1 (2007).
[245] David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1370 (1996).

computer systems in many countries before attacking the target as illustrated in chapter two.[246] Such a difficulty leads to making the territorial jurisdiction base less relevant in the context of cybercrime.[247] Third, unlike the traditional crimes that usually happen within one state's territory, cybercrime has a transnational dimension as a cybercriminal can easily commit several offenses in many countries simultaneously so that it is not usually linked to a single state.[248]

Likewise, Phillip Kastner and Frederic Megret state that "It is evident that the territoriality principle, one of the principles on which national criminal jurisdiction is usually based, is only of limited use in the context of cybercrime. There may be no single *locus delicti* in the traditional sense; several offenders may act together yet from different locations; experienced crackers can route their activities through portals in jurisdictions without specific legislation; and digital evidence may be dispersed on servers located in different jurisdictions."[249]

At the international level, the drafters of Arab Convention recognize the weakness of territorial principle relating to cybercrime when they provided in Article (30/3) a detailed order of priority regarding the competing jurisdictional claims. They are as follows: (i) states whose security or interests have been disrupted by the offense; (ii) states in whose territory the offense was committed; and (iii) the state of nationality of the offender.[250] In sum, I contend that all of pre-mentioned arguments undermine the weight of cybercrime's location as a factor to be considered in the case of a positive conflict of jurisdiction between two or more states.

4. Interest of the State of the Offender's Nationality

The third suggested factor in this regard is the interest of the state of the offender's nationality. Actually, the universal acceptance of nationality principle as a base for asserting criminal jurisdiction has encouraged most of cybercrime national laws to

---

[246] See discussion *supra* notes 41, 43 .
[247] Jean-Baptiste Maillart, *supra* note 11, at 4.
[248] Susan W. Brenner, *supra* note 37, at 198.
[249] Philipp Kastner & Frederic megret, *International legal dimensions of cybercrime,* in RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 190, 201 (Nicholas Tsagourias & Russell Buchan eds., 2015).
[250] Arab Convention on Combating Information Technology Offenses*, supra* note 9, at 15.

extend their jurisdiction if the crime is committed by one of its nationals abroad as shown in detailed in chapter four of this study.[251]

In reality, I contend that, besides the arguments in favor of the application of the nationality principle as a well-established ground of jurisdiction,[252] the exercise of this basis is urgently needed in the case of cybercrime for several reasons. First, it allows the state of nationality to prosecute its national committing a cybercrime from a location which is not subject to the territorial sovereignty of any state or from unknown place upon the return back to home. Otherwise, this crime will not be punished. Second, it prevents the nationals of one country from travelling to another country to commit a cybercrime and returning back to his/her own state without the possibility of being prosecuted if the national law prohibits the extradition of nationals to a foreign state. Third, the criminal could welcome the exercise of such jurisdiction in order to be prosecuted in a legal system he knows.[253] Hence, I argue that this factor should have more importance in prioritizing the competing jurisdictional claims relating to cybercrime.

5. Interest of the State of the Victim's Nationality

The fifth factor that should be considered in deciding the state that will be granted the jurisdiction over cybercrime is the interest of the state of the victim's nationality. As illustrated in chapter four, a state may extend its jurisdiction over serious crimes committed abroad against one of its own nationals that is called the passive nationality principle and some national laws extend their jurisdiction to cover a cybercrime committed abroad against their nationals.[254]

Generally, the passive nationality principle has become an accepted base for exercising jurisdiction. In spite of that, it is still criticized due to the problems that arise as a result of its application.[255] Regarding cybercrime, this ground for asserting jurisdiction is found in a limited number of international or regional instruments in relation to

[251] See discussion *supra* note 114.
[252] See discussion *supra* notes 116-120.
[253] CEDRIC RYNGAERT, *supra* note 101, at 107.
[254] *See* discussion *supra* notes 134.
[255] *See* discussion *supra* notes 135-137.

cybercrime and few countries include this basis for asserting their jurisdiction in national laws.[256] In addition, the attacks against computer systems and data stored in them are usually not directed against individuals of a particular nationality.[257] Thus, I allege that this factor should have less relevance in prioritizing the concurrent jurisdictional claims between two or more states over a particular cybercrime.

6. Interest of the State whose Vital Interest(s) has been Affected by Cybercrime

The sixth factor that should be evaluated in deciding this conflict is the interest of the state whose one of its vital interest has been affected by the cybercrime. Nowadays, as discussed in chapter four,[258] protective principle is a well-established concept in international law that allow a state to extend its jurisdiction over a crime committed abroad by aliens which cause substantial harm to one or more of its vital interests in the national territory like the state's security and the integrity of its governmental functions. Regarding cybercrime, many international and regional instruments allow the states parties to impose their jurisdiction based on the protective ground. At the national level, several national laws can be applied based upon the application of protective principle as well. Therefore, I consider this factor as an important one with high weight among other suggested factors.

In reality, the cybercrime may negatively affect and cause extensive damage to more than one state and all of them could claim their jurisdiction over this crime based on the application of the protective principle. In such case, the crucial question here is to which affected country the exclusive jurisdiction over the crime should be given if the other suggested factors in this chapter are equal. In fact, it seems logical that the best jurisdiction in this case is the country that has suffered the most harm as a result of this cybercrime.

However, what is the metric that can be used to measure such harm? Actually, the prevailing opinion in this regard is that the harm should be assessed in the light of number of victims and their financial loss which should encompass the funds that the offender(s) defrauded or stole from them and any other reasonable cost to include the

[256] Comprehensive Study on Cybercrime, *supra* note 2, at 193-194.
[257] Henrik W.K. Kaspersen, *supra* note 189, at 21.
[258] *See* discussion *supra* Ch. 4.

cost of interruption of service, responding to the offense, restoring the data or repairing the affected system, conducting a damage assessment, and other relevant costs.[259]

Nevertheless, the metric of victims number and their monetary loss can be inadequate in measuring the harm in relation to some types of cybercrime such as economic espionage and stealing military technology from a state or the obstruction of its vital systems.[260] In several situations, it can be difficult to assess the amount of harm as many victims may not report the case so that a state may find it hard to illustrate the damages in its territory as a result of a cybercrime.[261]

7. Interest of Criminal Proceedings

In fact, one of the most important factors to be considered when deciding the state that will be granted the exclusive jurisdiction over cybercrime is the interest of criminal proceedings. This can be achieved by the most efficient legal system, among the competing jurisdictions, to prosecute and adjudicate a cybercrime in the manner that could secure a conviction in a fair trial.

Actually, the efficiency of the concerned legal systems can be evaluated according to several elements as follows: First, the availability of witnesses or experts to prove the crime or if they are aboard, the existence of an effective electronic system to allow them to provide their testimony remotely via video conference or other means of online communication. As well as, the availability of well-established system for their protection against the possible revengeful acts by the perpetrator(s).[262]

Second, the admissibility of evidence before the national court i.e. whether the evidence that could be collected from foreign authorities and Internet Service Providers will be legally accepted in the trial without any objection from the defendant.[263] Also, the

---

[259] Susan W. Brenner, *supra* note 37, at 200-01.
[260] Önder Kutay Şeker, International Regulation of National Cybercrime Jurisdiction 53, (unpublished thesis, University of Tilburg), http://arno.uvt.nl/show.cgi?fid=127475.
[261] Henrik W.K. Kaspersen, *supra* note 189, at 21.
[262] GUIDELINES FOR DECIDING 'WHICH JURISDICTION SHOULD PROSECUTE?, *supra* note 220, at 3.
[263] Gerard Coffey, *Resolving Conflicts of Jurisdiction in Criminal Proceedings: Interpreting Ne Bis in Idem in Conjunction with the Principle of Complementarity*, 4 New J. Eur. Crim. L. 59, 79 (2013).

applicability of the statute of limitations or other defenses that the defendant could raise.[264]

Third, the potential punishment according to the national law in the case of conviction after the completion of trial process. However, it is enough that the national law establishes an adequate penalty for such crime as there should not be any consideration to the more intensive sentence in the competing national laws.[265] Otherwise, this will result in obliging the states to make their penal laws much harsher in the manner which does not adequate with the seriousness of the crime.

Fourth, the availability of a higher technical capabilities that can assist in collecting the required evidence and conducting the needed analysis of data and information to discover all the offenders and determine the caused damages. Also, the existence of the required experience and skills at the law enforcement authorities with regard to computer forensic and cybercrime in the manner that qualifies them to conduct the investigation and prosecution with great efficiency.[266]

Fifth, the stage of development of the criminal proceedings in the competing states should also be taken into account.[267] In addition, there should be an evaluation whether it is possible to divide the prosecution of the concerned cybercrime case into separate cases in two or more jurisdictions where the perpetrators and victims exist without prejudice to the interest of criminal proceedings in each country. In fact, the investigation and prosecution process of complicated transnational crime will frequently lead to the possibility of a number of prosecutions in different jurisdictions.[268] Indeed, this solution is effective as it will encourage all forms of international cooperation between the concerned states especially the mutual legal assistance to enhance the criminal proceedings in each one of them.

---

[264] Susan W. Brenner, *supra* note 37, at 204.
[265] Önder Kutay Şeker, *supra* note 260, at 53-54.
[266] *Id* at 46.
[267] GUIDELINES FOR DECIDING 'WHICH JURISDICTION SHOULD PROSECUTE?, *supra* note 220, at 3.
[268] Gerard Coffey, *supra* note 263, at 79.

Sixth, if the criminal is already arrested, a sufficient consideration should be given to the location of the custody taking into account the efforts that have been undertaken in relation to the criminal investigation that lead to the apprehension.[269]

Hence, I argue that this factor should have more importance in prioritizing the competing jurisdictional claims relating to cybercrime. However, it is not an easy task to decide which national legal system is the more efficient and effective one among other competing jurisdictions for the legal proceedings against cybercrime. Indeed, one method that could help in this regard is the establishment of an international review mechanism to assist and evaluate the efficiency of a national legal system against cybercrime. A similar one exists in relation to the implementation of the United Nations Convention against Corruption.[270]

To further clarify, A sample hypothetical example can demonstrate how the pre-mentioned factors could be applied in a particular case. If there is a conflict of jurisdiction over the same cybercrime between the state of victim nationality (country A) and the state of the offender's nationality (country B). In such a case, there are two factors which will not be assessed or examined which are the interest of the state of territorial jurisdiction or the interest of state whose vital interests have been affected by the crime. That is because this conflict does not involve any of those two states.

However, there are three other factors which should be evaluated: the interests of victim, offender, and criminal proceedings. Therefore, if both countries A and B can equally achieve these interests effectively, country B should take the exclusive competence over the crime because the interest of the state of the offender's nationality is more relevant than the interest of the state of victim's nationality as seen above. On the contrary, if country A can achieve all or two of these interests better than country B, the priority should be given to country A. Finally, the decision should be reached after considering and examining the previously mentioned factors and can be taken by

[269] Henrik W.K. Kaspersen, *supra* note 189, at 21.
[270] United Nation Office on Drugs and Crime, Mechanism for the Review of Implementation of the United Nations Convention against Corruption—Basic Documents (2011), https://www.unodc.org/documents/treaties/UNCAC/Publications/ReviewMechanism-BasicDocuments/Mechanism_for_the_Review_of_Implementation_-_Basic_Documents_-_E.pdf.

a certain body established for such a purpose or by the concerned states themselves after conducting the negotiation.

Another instance is the *Love Bug virus* case,[271] unfortunately the perpetrator was a Filipino and committed his crime from the Philippines which refused his extradition to the United States of America or other requesting countries because his act was not a crime at this time according to the Philippine law. However, if the Philippines had a law which criminalizes such act. In this situation, there would be a positive conflict of jurisdiction between Philippines and other states including United States of America which affected negatively by this virus.

By applying my proposed solution to such conflict and after evaluating the pre-mentioned factors, the jurisdiction should be given to the United States of America. That is because each of those two countries would be considered as having a territorial jurisdiction because the virus was uploaded in the Philippines and downloaded in the United States of America. However, the latter would achieve the benefit of victims and criminal proceedings better than the former due to the well-established American legal system and the using of developed means of investigation against cybercrime. Whereas, the Philippines did not have these capabilities at this time. The Philippines only can achieve the interest of perpetrator who existed there and had an interest not to be extradited to a foreign state.

Therefore, the United States of America shall fulfill the interest of victims and interest of legal proceedings; Whereas, Philippines will only achieve the interest of preparators. Finally, the decision here should be taken on the basis of an aggregate balance of the examined factors. Therefore, the jurisdiction would be granted to the United States of America which fulfills many of these factors more than the Philippines.

One more example is the *McKinnon v United States case,*[272] which is one of the most controversial cybercrime cases in the recent years. The facts of this case were as follows: a Scotland resident in England hacked into the US Pentagon system and got

[271] See discussion *supra* note 34.
[272] ALISDAIR A. GILLESPIE, CYBERCRIME: KEY ISSUES AND DEBATES 30 (2016).

sensitive data and deleted several files which impaired particular parts of the US defense network from functioning. Then, the USA requested his extradition for committing several cybercrimes but he objected against such extradition by raising many arguments. First, a plea bargain offered to him by US officials amounted to undue pressure and an abuse of process. second, he could be prosecuted in England for his crimes. Third, he suffered from autism and his extradition to the USA would amount to ill-treatment within the meaning of article (3) of the ECHR. Even though, all these attempts were dismissed by the court which decided his extradition to the USA.

On October 2012, the UK's Home Secretary refused his extradition due to his serious illness and decided that he could be prosecuted in the UK. However, on December 2014, the Director of Public Prosecution closed the case because it would be difficult to prove his crimes as the evidence was in the USA which would not cooperate with any prosecution in the UK. As a result, the UK had custody of the perpetrator but had no evidence against his crime; Whereas, the USA had indeed evidence but had no offender. Surely, the USA will seek his extradition upon his travel to another country. Actually, this case shows the negative results of the failure to reach a solution in the case of concurrent jurisdictional claims between states over a cybercrime.

By applying my proposed solution to solve this conflict of jurisdiction between the UK and the USA, I find that the UK fulfills the interest of the state of the territorial jurisdiction as the hacking act was committed by the offender through a computer in England, the interest of the state of the offender's nationality as he had the Britain's nationality, the interest of the perpetrator who preferred to be prosecuted in the UK and raised several argument against his extradition to the USA as seen above.

Whereas, the USA achieves the interest of the victim which was a governmental American institution that asked for his prosecution in the USA to secure his conviction and seek for the adequate compensation, the interest of the state of the territorial jurisdiction as the hacking act was committed against governmental computer system in the USA and caused substantive damages to it, and the interest of the state whose one of its vital interests has been affected by the crime as the offender deleted several files which impaired particular parts of the US defense network from functioning and committed other illegal acts which affected negatively the US's national security.

Also, the USA achieves the interest of the criminal proceedings as there was already an investigation launched in the USA, most of the witnesses were existed in the USA, all of the evidence was in the USA, the US prosecutors were able to investigate and prosecute the case effectively in the manner which covers the full extent of the alleged criminality, the punishments for the alleged offences were harsher in the USA than the UK, the availability of a higher technical capabilities in the USA that can assist in collecting the required evidence and conducting the needed analysis of data and information to determine the caused damages. Therefore, the USA fulfills more of the suggested factors than the UK so that I argue that the jurisdiction should be granted to the USA.

In sum, this chapter has discussed the advantages and disadvantages of the different approaches to deal with the dilemma of how to prioritize among the competing jurisdictional claims. It concludes by arguing that such a dispute over competence should be resolved by a decision taken after the assessment and evaluation of several suggested factors to include the interest of victim, interest of the perpetrator, the interest of the state where the crime was committed, the interest of the state of offender's nationality, the interest of the state of victim's nationality, the interest of the state whose one of its vital interests has been affected by the crime, and the interest of criminal proceedings.

VI. Conclusion

Actually, the Internet has become one of the most important technological innovations in the recent years with a great positive influence on communications, financial transactions, and the operation of dozens of institutions around the world. However, such development in the use of the internet and computer technologies has increased the possibility of their misuse by committing the different forms of cybercrime such as the spreading of viruses as well as the unauthorized access to and illicit tampering with systems, programs or data. In addition, the traditional crimes like fraud, forgery, and theft can be committed with the assistance of or by means of computers, internet and related communications technologies.

In most cases, the commission of cybercrime is linked with the two main features. The first one is the transnational nature of this crime and the second feature is the difficulty in deciding where the cybercrime actually took place or identifying the identity of cybercriminal. In fact, such challenges make the tracing of cybercrime very difficult and time consuming for the law enforcement authorities. In addition, they have increased the need to enhance international cooperation through the effective response to the mutual legal assistance and extradition requests in order to smoothly collect the evidence from another jurisdiction or apprehend the offender who exist in a foreign country.

Furthermore, such cross-border dimension of cybercrime resulted in the adoption of an expansive approach in relation to the exercising of jurisdiction as a method to counter such extra-territorial crime. Therefore, jurisdiction over cybercrime can be asserted based on several grounds including territorial, active nationality, passive nationality, and protective principles. Such broad approach may lead to the dilemma of positive conflict over jurisdiction which may result in hindering the mechanism of effective international cooperation, violating the fundamental principle of *"ne bis in idem",* and causing the duplication of efforts taken by the law enforcement officials of the involved states.

Nowadays, there are three different approaches to deal with this issue. The first opinion favors the negotiation between the concerned states aiming at centralizing the criminal proceedings on one single country. The second view prefers the establishment of an

obvious and binding rule which decides the priority among the competing jurisdictional claims. Whereas, the third opinion supports the development of a guideline which includes non-exhaustive factors to be considered and evaluated to reach a decision which can solve this conflict.

I argue that the most effective solution is through the determination of certain factors to be considered and evaluated in order to decide the best jurisdiction to take the exclusive competence over the cybercrime according to the facts and merits of each single case and taking into account the transnational nature and other characteristics that distinguish cybercrime from the traditional crimes. Such proposed solution is better than the attempt to solve such conflict through negotiation between the concerned states without providing them with determined factors to be considered in reaching a decision in this regard.

I contend that such factors should reflect the interests of the different stakeholders in relation to cybercrime that include like any other crimes the victim(s), offender(s), and involved state(s) that can assert their jurisdiction over cybercrime based on any of the accepted grounds to include territoriality, active, passive, and protective principles. Thus, these suggested factors should include the interests of victim(s), perpetrator(s), the state where the crime was committed, the state of offender's nationality, the state of victim's nationality, the state whose one or more of its vital interests has been affected by the crime, and the interest of criminal proceedings as it is essential for achieving the benefit of all the stakeholders.

In addition, these factors should be exhaustive to allow the involved states to predict in advance to whom the jurisdiction could be granted if the dispute arises which shall surely assist in preventing the conflict at the very beginning or before its occurrence. Furthermore, these factors should have different value as many factors are more important than others according to the transnational nature and other characteristics that feature cybercrime. Finally, the decision is taken on the basis of an aggregate balance of all these factors i.e. the jurisdiction will be given to the country that can fulfill many of these factors more than others. This decision can be taken by the concerned states themselves or by an international body established according to an international

instrument with an obligatory mandate to issue a binding decision in the case of conflict between states over competence in cybercrime.