ADDIS ABABA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE STUDIES

School of Law Graduate Program

LL.M in Public International Law

Critical evaluation on the applicability of Territoriality Principle of International Criminal Jurisdiction on transnational cybercrime and its Challenges thereof.

A Thesis Submitted in Partial Fulfillment for the Requirements of LL.M.

Degree in Public International Law

By

Baraki Belay

Advisor; - Wondwossen Demissie (PhD)

June 2023

Addis Ababa, Ethiopia

Declaration

I Baraki Belay, hereby declare that this thesis is my original work, and it has never been presented in any other University. All source materials used in this work have been duly acknowledged.

Baraki Belay

Signature _____

Date 02/06/23

Advisor: **Wondwossen D. (PhD)**

Signature _____

Date 02/06/23

Approval Sheet

Baraki Belay's thesis entitled "*Critical evaluation on the applicability of territoriality principle of international criminal jurisdiction on transnational cybercrime and its Challenges thereof*" is approved by the undersigned members of the examining board.

Board of Examiners	**Name**	**Signature**
Advisor:	Wondwossen D. (PhD)	
Examiner	KinfeMichael Y. (PhD.)	
Examiner	Semenih K.(PhD.)	

Dedication

This thesis is dedicated to the memory of my beloved mother Aynadis Tenaw. Her unwavering love, support, and encouragement kept me going throughout my academic pursuits. Her untimely passing has left a void that can never be filled but I take comfort in knowing that her spirit lives in all that I do. She was my source of inspiration, and I will always carry her teachings with me. This is for you, Ema. May you rest in eternal peace.

Acknowledgments

First and foremost, all thanks and credit are deserved to Almighty God.

My courteous gratitude goes to my advisor, Wondwossen Demissie (Ph.D.), for his support, kindness, constructive comments, and guidance.

My heartfelt gratitude goes to my friend Weynshet Haile who has contributed enormous effort and motivation for the accomplishment of my thesis.

Finally, yet importantly, I would like to pay high regard to my family for their sincere encouragement and inspiration throughout my life.

Table of contents

Acronyms

APEC	Asia Pacific Economic Cooperation
AU	African Union
CCPCJ	Commission on Crime Prevention and Criminal Justice
CoE	Council of Europe
DoS	Denial of Service
ECOSOC	Economic and Social Council
EU	European Union
GCCS	Global Cooperation on Cyber Security
ICT	Information and Communication Technologies
INAC	International Network Against Cybercrime
INTERPOL	International Criminal Police Organization
IP	Internet protocol
ISP's	Internet service providers
MLATs	Mutual legal assistance treaties
OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
PCIJ	Permanent Court of International Justice
SEA	Syrian Electronic Army
TEL	Telecommunications and Information Working Group
UK	United Kingdom

UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention on Transnational Organized Crime
USA	United States of America
VPN	Virtual Private Network

Abstract

After the development of computer technology, human life has been positively and negatively affected. This change in human history influences Criminal Justice System with the coming of Transnational Cybercrime which uses a computer or other digital devices connected to the Internet as a tool for committing criminal offenses. There are competing interests and ideas regarding Cyberspace and, Sovereignty of States between the ones which consider Cyberspace as separate from any shadow of the State's Sovereignty and the others who propose that the space is under the State's Sovereignty and regulation with attributing some elements of the technology to a specific State's territory. The proposition for regulating Cyberspace developed as the international norm by recognizing that the Criminal act costs significant damages to States and institutions. Consequently, regulating Crime through international, regional, and domestic legislation comes to the scene. However, regulation of the computer system was never easier because of the transnational nature of the system and the criminal acts committed through it. In the way of regulating transnational Cybercrime, Territoriality Principles of Criminal Jurisdiction could be used to prosecute the perpetrator of transnational Cybercrime with both the subjective and objective aspects. However, due to the borderless nature of the Crime, two or more states might be claiming Jurisdiction in one specific Crime, resulting in conflict, and overlapping of Jurisdiction. Consequently, to avert these challenges, there are tests/theories developed to be considered for successful and legitimate regulation of the conduct. Despite this, there are some challenges faced while applying the territoriality principle of criminal Jurisdiction on Transnational Cybercrime which emanates from the unique feature of the Crime being borderless and policy decisions by States.

Keywords

Transnational Cybercrime, Territoriality Principle, Jurisdiction. Cyberspace

Chapter One

Introduction

1.1.Background of the study

Advances in digital technology and the planet's digitization have entirely revolutionized how people live and interact with one another. On the negative side, information technology provides new methods for offenders and continues to challenge the International Criminal Justice system.[1] Recent reports have shown that Global losses from Cybercrime reached nearly $1 trillion in 2020.[2] Moreover, expected to cost 10 trillion annually by 2025.[3]

In the meantime, there comes a growing concern about regulating transnational Cybercrimes. Following this, the world's first International Convention on Cybercrimes came into existence in 2001 between the Council of Europe (CoE) and States Parties to the instrument.[4] The instrument recognizes the threat faced by the Computer system and obliges party States to take legislative measures to establish Jurisdiction on the crimes.[5]Consequently, States may formulate laws that enable them to exercise Jurisdiction over transnational cybercrimes that could be claimed based on the territoriality principle of Criminal jurisdiction with both objective and subjective territoriality principles. [6]

United Nations Office on Drugs and Crime (UNODC)[7] has received increasing mandates from the General Assembly, ECOSOC (United Nations Economic and Social Council), and the Commission on Crime Prevention and Criminal Justice (CCPCJ) [8] to provide technical assistance and training to States to improve

---

[1] United Nations Conference on Trade and Development (2012), *Measuring the Impacts of Information and Communication Technology for Development*, page 1.

[2]Tonya Riley, *The Cybersecurity*, Washington post-2020 Dec.7, 2020, available on https://www.washingtonpost.com accessed 08 February 2021.

[3]Cybercrime Magazine (2020), *Special Report: Cyberwarfare in the C-Suite*. Steve Morgan (Eds), available on https://cybersecurityventures.com/hackerpocalypse-cybercrime-report- accessed 25 September 2022.

[4] As stated in European treaty series no 185, Explanatory Report to the Convention on Cybercrime Budapest, 23. XI.2001, The Convention and its Explanatory Report were adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001), and the Convention was opened for signature in Budapest, on 23 November 2001, on the issue of the International Conference on Cybercrime.

[5] *Each Party shall adopt such legislative and other measures as may be necessary to establish Jurisdiction over any offense established per Articles* 2 through 11 of this Convention 'The Convention stated specific crimes that could be committed through computer systems from Articles 2-11.

[6] Article 22, Convention on Cybercrime.

[7] Article 41 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World states Brazil, from 12 to 19 April 2010.

[8] The Commission on Crime Prevention and Criminal Justice (CCPCJ) was established by the Economic and Social Council (ECOSOC), in its resolution 1992/1, as one of its functional commissions, upon the request of General Assembly resolution 46/152. The Commission acts as the principal policymaking body of the United Nations in the field of crime prevention and criminal

National legislation and to build the capacity of national authorities to prevent, detect, investigate, and prosecute cybercrime.[9]

At a regional level, the Arab Convention on Combating Information Technology Offenses aims *to improve Cooperation between the Arab States in combating cybercrimes to protect the security, interests of the Arab States, and the safety of their communities and individuals*. The treaty also describes information technology, lists offenses and procedural provisions, and outlines the mechanisms of legal and judicial Cooperation between State Parties.[10]

Another regional instrument is the African Union Convention on Cyber Security and Personal Data Protection.[11]Though it does not explicitly address the jurisdictional issues of Cybercrimes, it sets an objective to establish a credible environment for the digital world and to fill the gaps that affect the regulation and recognition of electronic communication as well as to move against Cybercrime through promoting Harmonization, mutual legal assistance, Exchange of Information, and means of Cooperation.[12]

Even though, international and regional efforts are made to curb transnational Cybercrime and its possible effect on Society. The current Criminal Justice System has faced jurisdictional challenges while regulating Cybercrime through the territoriality principle.

1.2.Statement of the problem

International experience in regulating transnational Cybercrimes through Criminal Justice System has faced challenges regarding the procedure to prosecute the perpetrators. Since Crime has the unique nature of being borderless, it could be challenging to apply the territoriality principle of criminal Jurisdiction and legally empower States to claim Jurisdiction based on the territory in which the act is committed.[13]Furthermore, this unique nature of the Crime makes it more difficult for the prosecution to acquire Jurisdiction through the territoriality principles of Jurisdiction than traditional crimes. They can be committed from anywhere in the

justice. ECOSOC provided for CCPCJ mandates and priorities in resolution 1992/2 www.unodc.org/documents/commissions, accessed 14 February 2022.

[9] United Nations Office on Drugs and Crime. (2013, February). *Comprehensive Study on Cybercrime.* Draft. Ilias Bantekas & Susan Nash (2003), International Criminal Law, 2nd Edition, Cavendish Publishing Limited, page 3.

[10] League of Arab States, Arab Convention on Combating Information Technology Offenses, Dec 21, 2010 (entered into force Feb. 7, 2014).

[11] Adopted by the 23rd Assembly, Heads of States and Governments held in Malabo, Equatorial Guinea, in June 2014.

[12]Article 28, African union convention on cyber security and Personal Data Protection.

[13]Nadina Foggetti(2008), *Transnational Cybercrime, differences between national laws and development of European legislation: by repression?*, in Masaryk University Journal of Law and Technology, Fall, page 34.

globe outside the affected State boundaries, creating more significant challenges for law enforcement agencies.[14]

As a result, Criminal Justice System's effort to assume Jurisdiction on transnational Cybercrime towards prosecuting the perpetrator of the Crime has never been easier. Applicability of the territoriality principle of international criminal Jurisdiction, enshrined under the international and regional conventions, raise the conflict of Jurisdiction that could be characterized simply as a positive and negative conflict of Jurisdiction emanates when more than one country possibly exercise/claim jurisdiction and no States having legitimate Jurisdiction on the Crime respectively. [15]Besides, other challenges are observed due to the unique nature of the Crime being borderless and committed through computer systems.[16]

1.3.Literature Review

Since law regulating the computer technology is a contemporary development in legal study, there is a wide range of works of literature regarding transnational Cybercrime and the applicability of international principles of criminal Jurisdiction on transnational Crime.

Scholars' perception regarding the prevalent issues of jurisdictional challenges of transnational Cybercrimes extends from regulating the Crime through traditional criminal law to regulating Cybercrimes with the special laws intended to regulate such crimes.[17] Some scholars also propose the "*Virtual World Sovereign Independence Theory."*[18] *which* states that Cyberspace should be outside the control of the States and have the right to exercise its Sovereignty. Though it does not have the support of most scholars considering the threats crimes pose to the public interest.[19]

Among the literature on criminal Jurisdiction in Cybercrimes, *XiaobingLi*, and *Yongfeng Qin* presented an article at the *8th international congress on Information and communication technology* entitled "*Research on Criminal Jurisdiction of Computer Cybercrime* ."The article proposed five new principles claiming

[14] Ibid
[15] Meetali Rawat(2021), *Transnational Cybercrime: Issue of Jurisdiction*, International Journal of Law Management & Humanities, Vol. 4 Issue 2, page 265.
[16] Ibid
[17] United Nations Office on Drugs and Crime (2013), *Comprehensive Study on Cybercrime Draft,* page 78
[18]John Perry Barlow, A Declaration of the Independence of Cyberspace, 1996. states '*'Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.''*
[19] Kreiss, D. (2014). *A Vision of and for the Networked World: John Perry Barlow's Declaration of the Independence of Cyberspace at Twenty.* In J. Bennett, P. Kerr, and N. Strange (Eds.), Media Independence: Working with Freedom or Working for Free? New York, NY: Routledge, page 112.

Jurisdiction on Cybercrime as follows: *Theory of new Sovereignty, Theory of Jurisdictional relativity, Theory of website jurisdiction, Principle of limited Jurisdiction, and Principle of minimum contact*. And it has been concluded that the application of these principles results in the conflict of Jurisdiction as well as the conflict results in the impunity of the perpetrator of the Cybercrime.[20]

There is also a comparative study made to evaluate the adequacy of the present laws and principles as to criminalizing and asserting Jurisdiction on transnational Cybercrimes and states that the present principles/laws are inadequate and unable to regulate Cyberspace successfully. [21] Furthermore, they claimed too much dependence on the territorial principle of Jurisdiction, which is hard to apply considering the unique nature of the Crime and the need to apply an extraterritorial principle to claim specific Jurisdiction. Besides, traditional laws that do not exhaustively and specifically regulate Crime have posed severe problems in the ongoing process of prosecution and exercising Jurisdiction.[22]

An article entitled "*Overcoming the conflict of jurisdiction in cybercrime*" *by Abdelmonem Mohamed* states that the conflict of Jurisdiction in the application of international criminal jurisdiction principles results from the extensive International, Regional, and National regulation of Cybercrime and elaborates that this conflict of Jurisdiction could be resolved through three possible approaches. The First approach is, based on negotiation and mutual assistance between the concerned States. The Second one is, laying down standards regarding which principle of Jurisdiction should be given priority over the other principles when there is overlapping Jurisdiction. Moreover, the third approach states that there is a need to have factors/standard guidelines to be considered to reach a decision that could solve the conflict of Jurisdiction.[23]

This research intends to critically evaluate the applicability of the territoriality principle of criminal Jurisdiction in asserting Jurisdiction on transnational Cybercrime and its challenges.

[20] Jun Li and Jidong Jia(2018), *Confusion and Relief of Criminal Jurisdiction of Cybercrimes*, School of Law, Huazhong University of Science and Technology, page 4.
[21] Qianyun WangA (2016), *Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*, Erasmus University Rotterdam, page 14.
[22] Ibid
[23] Khalifa, Abdelmonem (2020). *Overcoming the Conflict of Jurisdiction in Cybercrime*. American University in Cairo, Master's thesis. AUC Knowledge Fountain, page 67.

1.4.Objective of the Study

1.4.1. General objective of the study

The main objective of this study is to evaluate the applicability of the territoriality principle of international criminal Jurisdiction to transnational Cybercrimes.

1.4.2. Specific objectives of the study

The study specifically aims:

- To examine the relevance of the territoriality principle in asserting Jurisdiction on transnational Cybercrime.
- To examine the possible challenges in asserting Jurisdiction based on the territoriality principle on transnational Cybercrime.
- To measure the extent of applicability of the parameters used to claim Jurisdiction and resolve a conflict of Jurisdiction based on the territoriality principle.

1.5.Research Questions

- To what extent the territoriality principle is relevant in asserting Jurisdiction on transnational Cybercrime?
- What parameters are used to claim Jurisdiction on transnational Cybercrimes through the territoriality principle of Jurisdiction?
- What are the challenges and possible solutions in applying the parameters to acquire Jurisdiction based on the territoriality principle?

1.6.Significance of the Study

The study will have an enormous role in understanding the applicability of the territoriality principle of international criminal Jurisdiction and the factors to be considered in acquiring Jurisdiction through the territoriality principle in prosecuting transnational Cybercrime and its challenges.

1.7.Research Methodology

The research will be conducted as desktop research by analyzing the laws and practical cases from different jurisdictions related to the issue under discussion. It will be based on both primary and secondary resources. To assess the extent of applicability of the territoriality principle, international and regional instruments,

different countries' laws on Cybercrime, and well-established Customary International law on the principles of international criminal Jurisdiction, the UN General Assembly resolutions and cases related to transnational Cybercrime will be employed as the primary source. Books, Journal articles, and other written commentaries on the legislation and case laws will also be used as Secondary resources. Additionally, reports, websites, and the relevant Countries experiences will be consulted to assess the challenges in the applicability of the territoriality principle in transnational Cybercrimes.

1.8.Organization of the Paper

The paper will be composed of five chapters. The first chapter will deal with what, why, and how the research is conducted; simply, it is the research proposal.

The second chapter will be about an introductory remark on transnational Cybercrime, the international, regional, and domestic legal frameworks on transnational Cybercrime, and the territoriality principle of criminal Jurisdiction.

The third chapter will be about the general overview of the International criminal law territoriality principles on acquiring Jurisdiction and its applicability to transnational Cybercrime.

The fourth chapter will discuss the challenges of the applicability of the territoriality principle on transnational Cybercrime.

The last chapter will be the concluding remarks and recommendations.

Chapter Two

Transnational Cybercrime and the International Legal Framework

2.1. Overview of Transnational Cybercrime

In the 1970s, criminals began using the new technology for illicit activity. The first *ransomware*, malicious software that encrypts and locks a user's data until a ransom is paid, was recorded. [24] The birth of web browsers and email was widely available in the 1990s and came to provide a new tool for Cybercriminals to exploit. [25]As a result, they could increase dramatically and reach out and scam individuals from afar. Then the decade of the 2000s comes with the emergence of social media, which makes the commission of Cybercrime much easier.[26] On the other hand, it makes regulating Criminal activities much more complicated than before. Consequently, it gets the attention of the international community.[27]

The age of globalization has provided unprecedented opportunities for participation in the global economy and personal expression. It has also created new avenues/modalities for Criminal activity.[28] Transnational Cybercrime has become a new extending problem in the Criminal Justice System, and it includes crimes directed at Computers, inter alia hacking or denial of service (DoS) attacks through the computer system as online fraud, identity theft, and the distribution of child exploitation materials. United Nations Office on Drugs and Crime (UNODC) has estimated that identity thieves steal $ 1 billion annually globally, and online retailers lost $ 3.5 billion because of fraud in 2012.[29]

Cybercrime could cover a wide range of offense committed directly or indirectly through the computer system. To further elaborate, we may consider four types of cybercrime; offenses against the *confidentiality, integrity, and availability of data and information systems*. [30]where the computer system is used to commit a crime, though not an essential one for the commission of a crime, when content-related offenses, pornography, and acts of a racist and xenophobic nature. These acts fall within the category of Cybercrime

[24]Wall, D (2001), *Crime and the Internet Crime, cybercrime and cyber-fears*, 1st edition, Routledge., Page 4.
[25] Ibid
[26] Ibid
[27] Ibid
[28] Wall, D. (2007). *Cybercrime*: *The transformation of Crime in the information age. Polity*: Cambridge University Press. Page. 44
[29] Ibid
[30] Calderoni, F. (2010). *The European legal framework on Cybercrime: striving for effective implementation*. Crime, Law and Social Change, 54(3), page 4.

when they are committed through a computer system and copyright infringement, as in the unauthorized copying and sale of computer software.[31]

In 1995 the UN Convention on Transnational Organized Crime defined an offense as a transnational crime when the Crime has been committed in multiple States, significant roles have been undertaken in different States as in one State's preparation, planning, direction, or control, the Crime was committed in one State but involved an organized perpetrator that commits the crimes in other states and, the Crime was conducted in another State but had significant impacts there.[32]Additionally, considering the complex nature of the Crime as one that takes place in the borderless realm of Cyberspace, the UN currently lists transnational Cybercrime as one of the major transnational crimes.[33]

2.2. The International Legal Framework on the Transnational Cybercrimes

Cognize of the threat posed by Transnational cybercrime, there is a need to regulate transnational Cybercrime. To this effect, the international community is moving towards formulating international and regional legal frameworks for regulating transnational Cybercrime.

The first comprehensive international effort was initiated in 1983 by the Organization for Economic Cooperation and Development (OECD) to deal with the criminal law problems of Cybercrimes.[34] Furthermore, the organization conducts a study to achieve the international Harmonization of Criminal laws to address Computer-related crimes. Based on the studies, the Organization recommended that member Countries consider the extent to which knowingly committed acts of Computer-related abuse should be criminalized and covered by national penal legislation.[35] Furthermore, the study resulted in a report which surveyed existing laws and proposals to be reformed. It recommended a minimum list of abuses that countries should consider penalizing by criminal law. Besides, it requests that Member States establish adequate penal, administrative, or other sanctions for misuse and abuse of information systems.[36]

---

[31] Osman Goni(2022*), Cyber Crime And Its Classification*, International of Electronics Engineering and Applications, Vol. 10, No.1, page 2.
[32]Wilson, K. (2020). *Transnational Crime*. In Alexander Lautensach & Sabina Lautensach (Eds.), International Criminal Law: Cases and Materials, 2nd Edition, Oxford University Press, page 413.
[33] Resolution adopted by the General Assembly on 21 December 2010, para 9.
[34] Ana Cerezoa, Javier Lopez and Ahmed Patel, *International Cooperation to Fight Transnational Cybercrime*, Conference Paper, September 2007, page 13.
[35] Ibid
[36] Ibid

On the other hand, UNGA has adopted several resolutions since 2000-200l to initiate a study on the problem of Cybercrime and possible response to it.[37] Moreover, it has also adopted a resolution to combat the criminal misuse of information technologies. It also provides that States should ensure their laws and practices eliminates safe environments for the perpetrator of criminal conduct through misuse of information technologies.[38] States should protect the *confidentiality, integrity, and availability of data* and Computer systems from unauthorized access and impairments and ensure that criminal violations are penalized.[39]

Despite the concern about the global challenge regarding transnational Cybercrime, there has yet to be a universal agreement on how to tackle Cybercrime at the global level or a common understanding of the definition of what cybercrime constitutes. From the perspective of human rights, it is essential to keep the scope of any convention on cybercrime narrow. Furthermore, expansive cybercrime laws may have the effects of adding up punishments due to the use of a computer system in the commission of an existing offense and compromise the protection of human rights.[40]

Having seen the international community's understanding and moves toward the need for a regulatory framework on transnational Cybercrime. There are some major regional and international conventions concerning Cybercrime for this research. In the next section of the paper, the researcher will discuss the three conventions, namely, Convention on Cybercrime (2001) and its additional Protocols, The African Union Convention on Cyber Security and Personal Data Protection, and Arab Convention on Combating Information Technology Offences.

2.2.1. Convention on Cybercrime (2001) and its additional protocols

In the 1997, Council of Europe (CoE) established a committee of experts to draft a Convention that would facilitate international Cooperation in the investigation and prosecution of Cybercrimes considering the unique nature of the Crime. Following this, in 2001, a final draft of the Convention was completed and adopted by the CoE, Committee of Ministers. It was also open for signature to members of the Council of Europe and observer Nations, inter alia the United States. [41]

---

[37] General Assembly resolution 65/230 Twelfth United Nations Congress on Crime Prevention and Criminal Justice, para 9.
[38] General assembly resolution 55/63. Combating the criminal misuse of information technologies, para1(a).
[39] Ibid
[40]H.E. Ms. Faouzia Boumaiza Mebarki, *Letter to the UN Ad Hoc Committee on Cybercrime, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose*, accessed on https://www.hrw.org/news/2022/01/13/letter-un-ad-hoc-committee-cybercrime 19 October 2022.
[41] Ibid n 13

The Convention's main objective is to adopt a standard criminal policy to protect society against Cybercrime, especially by adopting appropriate legislation and enhancing international Cooperation.[42] It came into force by the Council of Europe in 2004 as the first Intergovernmental Treaty Organization to deal with Cybercrimes. More specifically, concerning *infringements of copyright, computer-related fraud, child pornography, and violations of network security*.[43]It has been assumed to assist in the convergence, consistency, and compatibility of cybercrime legislation between Countries and guided developing nations toward best practices in drafting their cybercrime legislation.[44]

It is supplemented by two additional Protocols,[45] One that makes '*any publication of racist and xenophobic propaganda via computer networks a criminal offense'* and separates from the Convention. The terms of the Protocol would not bind a country that signed and ratified the Convention but not the Protocol. [46] The other additional Protocol on Cybercrime Enhanced Cooperation and Disclosure of electronic evidence aims to bring the Budapest Convention up to date with current technological challenges.[47]

Article 22, paragraph 1 of the Convention recognizes the applicability of the territoriality principle of criminal Jurisdiction. Accordingly, article 2 through 11 of the Convention states that Cybercrimes that have occurred in *the territory of one Party, in a ship flying its flag or in an aircraft registered under its laws, is to be prosecuted in that State*.[48] Consequently, the Convention provides that States where the person attacking a computer system and the attacked system are located within its territory could easily assume Jurisdiction based on the territoriality principle. It will also be applicable when the attacked computer system is within a States Party's territory, even if the attacker is in another Country.[49]

---

[42] Mohamed Chawki, A *Critical Look at the Regulation of Cybercrime a Comparative Analysis with Suggestions for Legal Policy*, Page 8.
[43] Ibid
[44] Ibid
[45] First, the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (28 January 2003), and Second Additional Protocol to the Convention on Cybercrime on enhanced Cooperation and disclosure of electronic evidence (17 November 2021).
[46] Ibid
[47] Ibid
[48] Armando A. *Cottim (2010), Cybercrime, Cyberterrorism, and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime*, European Journal of Legal Studies, 2010, vol 2, issue 3, page 12.
[49]Veridiana Alimonti,(2022) *Assessing New Protocol to the Cybercrime Convention in Latin America: Concerns, Human Rights Considerations, and Mitigation Strategies*, Electronic Frontier Foundation, page 4.

Furthermore, the Convention allows domestic laws to provide additional constituent elements. It provides the possibility of a reservation and also fully respects member states' decision-making on criminal policy.[50] On the other hand, this diversified implementation will decrease the consensus on the harmfulness of conduct and increase the possible obstacles to international actions. The negative effect of this kind of provision is expected to diminish the effectiveness of prolonged, expensive international negotiation for an agreement.[51]

2.2.2. The African Union Convention on Cybersecurity and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection was adopted by AU general assembly in 2014 during the 23rd Assembly held in Malabo based on the continent's need to adhere to the legal and *regulatory requirements on electronic transactions, cyber security, and personal data protection*.[52] It addresses the challenges posed by criminal activities committed over ICT networks in a manner relevant to regional and Continental specificities and in response to the need for harmonized legislation in the cyber security and personal data protection field. The Convention aims to set up basic rules for establishing a modern information society and secure Cyberspace in Africa by addressing the need for harmonized cyber legislation to facilitate Cooperation among the Member States of the African Union.[53]

The Convention seeks the establishment of a comprehensive Continental Legal Framework that sets broad guidelines for electronic transactions, personal data protection, and cyber security to prevent Cybercrime in African Cyberspace.[54] Embodies the existing commitments of African Union (AU) Member States at Sub-regional, regional, and international levels to build an information society that respects the cultural values and beliefs of the African Nations and guarantees a high level of legal and technological security to ensure respect of privacy and freedoms online while enhancing the promotion and developing Information and Communication Technologies (ICT) in the AU Member States. Furthermore, it sets out the essential security principles for establishing a credible digital environment to reduce the risks of Cybercrime and abuse of

[50] Article 42, Convention on Cybercrime.
[51] Ibid n45
[52] Fotso, O., Yagan, S, Ryu, E., & Choo, K. R. (2016). *Examining Cybercrime and cyber security trends in Africa*. Journal of Cybersecurity, 2(1). page 84.
[53]Ibid
[54] Ibid

personal data.[55]Moreover, a principle in international Cooperation is to curb the problem transnational Cybercrime faces.[56]

It also has a limited scope of application concerning data in the territory of a State Party of the African Union. Additionally, oblige the Party States to ensure the existence of a legislative framework to assist the investigation by authorities and make criminal liabilities. Despite this, the Convention does not deal with the applicability of the territoriality principle in the case of transnational Cybercrime. [57]

2.2.3. Arab Convention on Combating Information Technology Offences

In 2010, Arab Convention on Combating Information Technology Offences came into force to enhance Cooperation between Arab Countries, to combat information technology offenses threatening their security, interests, and the safety of their communities, and to enable Parties to adopt a standard criminal policy aimed at protecting the Arab society against information technology offenses.*[58]* Moreover, it aims to strengthen Cooperation between States to defend and protect their property, people, and interests from cybercrime.[59]

The Convention provides a broader range of crimes than the Budapest Convention in a specific stipulation. It includes the offense of illicit access, interception, against the integrity of data, misuse of information technology, forgery, fraud, pornography, and offenses related to terrorism, organized crime, copyright, and adjacent Rights and illicit use of electronic payment tools.[60]

Article 30 of the Convention provides that the State party should adopt necessary procedures for the following cybercrimes when they are committed in the territory of the State Party. Second, when committed on board a ship raising the *flag of the State Party or on board a plane registered under the law of the State Party*.[61]Third, an offense committed by a national of the State Party and punishable by domestic law in the

---

[55] Uchenna Jerome(2019), *The African Union Convention on Cyber Security: A Regional Response towards Cyber Stability, Masaryk* University Journal of Law and Technology, vol. 5, no. 1, page 92.
[56] Article 28, African Union Convention on Cyber Security and Personal Data Protection, Addis Ababa, Ethiopia, April 8-11, 2019.
[57] Article 9(c) and Section 2 African Union Convention on Cyber Security and Personal Data Protection.
[58]Afnan Alabdulatif (2018), *Cybercrime and analysis of Laws in Kingdom of Saudi Arabia*. Master of Science in Information System Security Faculty of the Department of Information and Logistics Technology University of Houston, page 54
[59] Ibid
[60] League of Arab States, Arab Convention on Combating Information Technology Offenses 5-9, Dec. 21, 2010 (entered into force Feb. 7, 2014)
[61] Shqair, Y. (2020). *Cybercrime Laws in Arab Countries Focus on Jordan, Egypt, and the UAE.* Fredrich Naumann Stiftung, Page 40.

location where it was committed or when it was committed outside the Jurisdiction of any State. Fourth, when the offense affects an overriding interest of the State.[62]

Aside from the International and Regional instruments relating to transnational Cybercrime, some International Treaties are not directly made to the regulation of Cybercrime. However, they are relevant in the regulation of transnational Cybercrime. The United Nations Convention on Transnational Organized Crime (UNTOC), along with other Treaties, deals with transnational Organized Crime and shows the United Nations' commitment to combat transnational Cybercrime when they are committed in an organized form.[63]

No provision in UNTOC defines Cybercrime. Instead, it can be covered under its articles when Cyberspace is used as an environment for committing Organized Crimes.[64]Furthermore, Section 3 of the UNTOC states that an offense is transnational when it is committed in more than one State when committed in one State. However, a substantial part of its preparation, planning, direction, or control takes place in another State, when committed in one State but involves an Organized Criminal Group that engages in criminal activities in more than one State and when committed in one State but has substantial effects in another State.[65]

The Convention on Protection of Children against Sexual Exploitation and Sexual Abuse is also known as Lanzarote Convention,[66] explicitly prohibits the dissemination of continents of child abuse and prostitution through the computer system.[67] Furthermore, Article 25(1) of the Convention provides that Jurisdiction could be established for offenses committed on a *Party's territory, a ship flying the flag of that Party, on board an aircraft registered* under the laws of that Party, by one of its Nationals or by a Person who has his or her habitual residence in its territory.[68]

In addition to the international legal frameworks adopted at the international and regional level, considering the harmful effect the acts could have on society. Our Country, Ethiopia, has promulgated the 2004 Criminal Code.[69]Moreover, the justification for the penal code amendment aimed to address crimes born of

---

[62]Ibid
[63] Ilias Bantekas & Susan Nash (2003), *International Criminal Law*, 2nd Edition, Cavendish Publishing Limited, page 50.
[64] Ibid
[65] Ibid
[66] Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse Lanzarote, 25.X.2007.
[67] McCusker, R. (2007). *Transnational organized Cybercrime: Distinguishing threat from reality*, Springer Science + Business Media B.V, page 270.
[68]Ibid
[69] Proclamation No. 414/2004, *Federal Negarit Gazeta,* Addis Ababa, 9th May 2005, here in after as the FDRE criminal code.

technological advancements, such as computer crime.[70] However, The Code has devoted only six articles (Articles 706-711) under section II of 'Property Crime' in Book IV for Cyber related crimes. Under these provisions, *accessing, accession, and taking or using data; accessing and deleting or altering; or denying services on Computers, Computer systems, and Computer networking intentionally or negligently constitute Computer crime* are included. [71]

The Code also states that as per article 710, *"Where one of the other crimes provided; fall under this Code is committed through a Computer, the relevant provision shall apply*.''[72]Therefore, we can prosecute ordinary crimes committed through the computer. Despite the provision being part of Property Crimes, the code will not impede the law from regulating other non-property Cybercrimes.[73]On the other hand, the Criminal Code has incorporated the territoriality principle of criminal Jurisdiction as per Article 11 of the code that anyone could be criminally liable for the violation of a provision provided under the code if he/she performed the act within the territory of Ethiopia irrespective his/her nationality.[74]

Additionally, Article 25(2) *non-instantaneous* crimes that recognize the scenario in which the act and the criminal result/effect do not coincide, the Crime is deemed to have been committed both at the place of the unlawful act and that of its result. [75] Through the above principle and legal provision, the prosecutor may find a way to charge perpetrators of transnational Cybercrime committed on Ethiopia territory or have resulted in effect in Ethiopia territory.[76]

Specific legislation regarding computer crime came to exist in 2016 and was justified by the insufficiency of the existing law for prosecuting computer crimes. [77]The proclamation categorizes computer crimes into three. Those are; crimes committed against the computer system, Computer Data, or Computer network,

[70] Cybercrime, or computer-oriented Crime, is a crime that involves a computer and a network. The computer may have been used to commission a crime or be the target (2002). computer forensics: incident response essentials. Addison - Wesley.)https://www.internetsociety.org/blog accessed on February 2, 2022
[71] Ibid
[72] Article 710, FDRE Criminal Code of Ethiopia.
[73] Ibid
[74] Article 11, FDRE criminal code of Ethiopia.
[75]Article 25(2), FDRE criminal code of Ethiopia.
[76] Ibid
[77]Computer crime proclamation no 958/2016, 22nd Year No. 83 Addis Ababa 7th July 2016, here in after as computer crime proclamation

Conventional Crimes committed through a computer, and illegal Computer content data disseminated through a computer, Computer system, or Computer network.[78]

Furthermore, the proclamation introduces the new concept of Service Provider liability. As per Article 16, the service provider shall be criminally liable for any illegal[79] computer content data disseminated through its computer systems by third parties., when it is directly involved in the dissemination or editing of the contents of data. Second, actual knowledge about the illegality of the data exists and failure to take any measure to remove or restrict access to the content data upon obtaining notice from competent administrative authorities.[80] Despite this, Ethiopia is not a signatory to any major international and regional instruments on Cybercrime.[81]

In addition to the legislative framework discussed at the international and regional level, there are institutional setups to combat transnational Cybercrime. At the international level, United Nations and European Union have significantly worked towards curbing the challenges of transnational Cybercrime by outlining policies and strategies involving their sub-Committees and Organs. More specifically, they were working on the Criminalization of the act and Harmonization of the Criminal law as well as Cooperation in enforcing the international instruments regarding transnational Cybercrime.[82]

At the regional level, apart from the above legal frameworks discussed in the previous section, Asia-Pacific Economic Cooperation (APEC) comprises 21(Twenty-one) members that form the Pacific Rim and carry out activities to prevent Cybercrime to promote economic growth and fight terrorism through its Telecommunications and Information Working Group (TEL) which undertakes cybersecurity legislation and enforcement capacity-building project for its Members.[83]

[78] Article 2(1), Computer crime proclamation
[79] Refers to provisions 12 to 14, including dissemination of advertisement through computer systems, crimes against public security, obscene or indecent crimes committed against minors, crimes against liberty and reputation of person
[80] Article16, Computer crimes proclamation
[81] Iyasu Teketel(2018), *Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences,* A Thesis Submitted to the School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Masters of Law (LL.M) in Public International Law Stream, Page 63.
[82] Cristos Velasco (2022), *Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments,* ERA Forum, page 115.
[83] Neethu N(2020), *Role of International Organizations in Prevention of Cyber-Crimes*, the Nalsar University of Law Hyderabad, Page 14

Another regional organization on the issues of transnational Cybercrime is the Organization of American States (OAS), comprising 35(Thirty-five) Member States in the North and South American Continents. The organization of the American States was established to promote solidarity and collaboration in the American continent through its intervention and computer security incident response teams established in its member states.[84]

On the other hand, in terms of an enforcement and professional perspective, International Criminal Police Organization (INTERPOL) has a core mission to enable law enforcement agencies in its 190 Member Countries to work together to combat transnational Crime, inter alia Cybercrime and also serves as a center for Information Exchange and Intelligence sharing, and provides technical expertise, training, and capacity building.[85]It has developed two secure platforms to facilitate Cybercrime related communication among police, namely the *Cybercrime Knowledge Exchange Workspace And The Cybercrime Collaborative Platform Operation*.[86]

Having an overview of transnational Cybercrime, International and Regional legal framework followed by some points about the Ethiopian framework and international Institutions towards regulating transnational Cybercrime through Criminal Justice System. The next chapter will be about the applicability of the territoriality principle of International Criminal Jurisdiction on transnational Cybercrimes.

[84] Ibid
[85] Prof. Dr. Kennedy Gastorn (2017*), Relevance of international law in combating cybercrimes: current issues and AALCO'S approach*, Presentation at the 4th World Internet Conference, page 10.
[86] Ibid

Chapter Three

Applicability of Territoriality Principle of International Criminal Jurisdiction on Transnational Cybercrimes

3.1. Territoriality Principles of International Criminal Jurisdiction

The territorial principle of international criminal Jurisdiction applies to crimes committed within the territory of a State that may come before the Court of the concerned State. It applies its laws without considering the perpetrator's nationality. This principle emanates from the logical deduction of the independence and Sovereignty of States for the maintenance of law and order within their territory.[87]Hence, the State has the lawful authority to exert control within its territory without other States' authority to govern. This extends to a decision to characterize certain acts as lawful or unlawful by the criminal law and enforces the law when it is violated within the territory. The result affects the territory of another State. [88]

The emergence of the principle of territorial Jurisdiction can be traced back to the Lotus case in public international law. The case arose from a collision between a French and a Turkish vessel in international waters. The Turkish authorities arrested the French officer responsible for the collision, and France challenged Turkey's right to exercise Jurisdiction over a French national in international waters.[89] The Permanent Court of International Justice (PCIJ), in its decision on the Lotus case, stated that in the absence of a rule of international law to the contrary, Turkey was entitled to exercise Jurisdiction over the French officer because the incident occurred outside of French territory and did not violate the principle of territoriality.[90]

Furthermore, the decision affirmed the principle of territorial Sovereignty, which holds that States have exclusive Jurisdiction over their territory and may exercise their powers of Jurisdiction over individuals and vessels within their territorial boundaries. Moreover, a State cannot exercise any power outside its territory except by a permissive rule derived from Customary international law or Conventions.[91]

The principle of territoriality reflects the exclusive responsibility and right of the States to adjudicate the case within the territorial limit, which includes land, sea, and air. Besides, there is a clear presumption in favor of

---

[87] Malcolm Shaw (2008), *International Law*, Cambridge university press, Sixth edition, page 1206.
[88] Brenner, Susan (2005), *Approaches to Cybercrime Jurisdiction*, Journal of High Technology Law, page 7.
[89] Lotus (France v. Turkey), PCIJ series A, no. 10, p. 4 (1927).
[90] Ibid
[91] Jan Kleijssen and Pierluigi Perri(2017),*Cybercrime, Evidence and Territoriality: Issues and Options*. Kuijer and W. Werner (eds.), Netherlands Yearbook of International, T.M.C. Asser Press page 155.

the Jurisdiction of the territorial State as the most convenient forum, given that the accused, witnesses, evidence, and victims will almost always be located on that territory.[92]

The principle could guarantee Jurisdiction in two major ways with Subjective and Objective territoriality Principles of International Criminal Jurisdiction. The former applies when an act that violates the law takes place within the territory of the forum State, in which case the forum State has the Jurisdiction to try the case. In the latter, a State is entitled to try criminals for offenses committed elsewhere. However, its effects result in the forum State's territory, and the forum state could have Jurisdiction Despite the act being performed in another State's territory. [93]

Exclusive Jurisdiction of one State over a crime is incompatible with the exercise of Jurisdiction over a crime involving more than one state in its commission. In case when the territory in which the criminal act is performed, and effects of criminal activities occur in different States. Consequently, this might result in overlapping Jurisdiction between States who assume Jurisdiction based on Objective and Subjective territoriality principles.[94]

3.2 Transnational Cybercrime and Territoriality Principle of International Criminal Jurisdiction

The territoriality principle of international criminal Jurisdiction requires the characterization and prosecution of criminal conduct, which must have a territorial nexus to the Jurisdiction in which it was committed. This is an essential principle for nation-states looking to assert their Sovereignty over criminal behavior occurring on their soil. However, it presents unique challenges to enforce this principle because of the borderless nature of Cyberspace and the ability of perpetrators to operate from it.[95]

In this regard, the US Supreme Court also ruled that the character of an act as lawful or unlawful is determined by the law of the Country where the act is done, and no State could apply its criminal laws to conduct within the physical territory of another State.[96]However, the development of information technology comes up with criminal acts accompanied by the unique features of Cyberspace, which could be considered an arena for the

[92]Gideon Boas (2012), *Public International Law Contemporary Principles and Perspectives,* Edward Elgar Publishing Limited, page 245.
[93] Ibid n 66
[94] Rollin Perkins (1971), *The Territorial Principle in Criminal Law*, Hastings L.J. Page 1159.
[95] Wendell Berge (1931), *Criminal Jurisdiction and the Territorial Principle*, Michigan Law Review, The Michigan Law Review Association Vol. 30, No. 2, page 240.
[96] American Banana Co v. United Fruit Co., 213 US 347 (1909).

commission of transnational Cybercrimes and allow the crimes to be committed outside the territory of the State different from the territory which the effect of the criminal act has occurred and make the applicability of the territoriality principle complicated.[97]

In response to this complication, States and international law enforcement agencies have developed treaties to help coordinate their efforts in investigating and prosecuting Cybercrimes across borders. For instance, the Budapest Convention on Cybercrime provides a framework for Cooperation among countries to investigate and prosecute Cybercrimes, regardless of where they may have occurred.

3.2.1. Cyberspace and State Sovereignty

Before assessing the applicability of territorial principles of criminal Jurisdiction on transnational Cybercrime, there is a need to discuss the concepts of territorial Sovereignty and Cyberspace Since they are the bases for the principle of Jurisdiction and the environment for the commission of the Crime.

Cyberspace is *a 'global domain within the information environment consisting of the interdependent network of Information Technology infrastructures, including the Internet, Telecommunication Networks, Computer systems, and embedded processors and controllers*.' [98] It is also the environment created by the connections of a Cooperative Network of Computers, information systems, and Telecommunication infrastructures, which could be called the World Wide Web.[99]

There are two major arguments regarding the inter-relationship between Cyberspace and the Sovereignty of States. The first line of argument leads by John Barlow, who promulgated the Declaration of the Independence of Cyberspace in 1996, claiming that Cyberspace is an independent dimension outside the reach of rules and regulations of other human spheres. Consequently, Cyberspace is viewed as *terra nullius*, a place not yet under the regulation of any Government, and no State has a cyber-territory.[100]

The second line of argument proposes that Cyberspace is an abstract dimension having physical locations and other attributed factors to connect with the Sovereignty of the State. Besides, the actors in Cyberspace

[97] Sunil. C. Pawar et al. (2021), *Cyber Crime, Cyber Space and Effects of Cyber Crime*, International Journal of Scientific Research in Computer Science Engineering and Information Technology, Volume 7, Issue 1, page 210
[98]Nicholas Tsagourias(2022), *The Legal Status of Cyberspace; Sovereignty redux*, Research handbook on international law and Cyberspace, Nicholas Tsagourias and Russel Buchan(Ed), Edward Elgar Publishing Limited, page 14.
[99] Ibid
[100] Ella Shoshan (2014), *Applicability of International Law on Cyber Espionage Intrusions*, Faculty of Law Stockholm University, page 22.

are also subjects of the State's Jurisdiction. This makes it clear that Cyberspace does not exist in a vacuum. Instead, the technology and the actors that constitute and effectuate Cyberspace are subject to State Sovereignty.[101]

Apart from the above contentions, many representatives of states in the international community agree with the applicability of international law on Cyberspace by overruling the idea that considers Cyberspace as having Sovereignty. In doing so, they set different connecting factors between the technology, State's territorial Sovereignty, and conducts within Cyberspace. [102]

US International Strategy for Cyberspace noted that the development of norms for State's conduct in Cyberspace does not require a reinvention of Customary International Law, nor does it render existing norms obsolete.[103] Furthermore, the UN Group of Governmental Experts, which includes Russia and China, agreed that international norms and principles that flow from Sovereignty apply to State conducts related to ICT, inter alia to Jurisdiction over ICT infrastructure within the States territory.[104]

UN Secretary-General also recommends that ICT security in the existing framework of international law and understandings that govern State relations provide the foundation for International Peace and Security. Therefore, the applicability of the principle of Territorial Sovereignty to Cyberspace entails that the Cyber-infrastructure located on the land territory, in the internal waters, in the territorial sea, and, where applicable, in the archipelagic waters or the National airspace is covered by the respective State's territorial Sovereignty. Hence, States are entitled to exercise control over the Cyber-infrastructure and activities on the infrastructure.[105]

Thus, the applicability of the principle of territorial Sovereignty in Cyberspace is the inherent right of the states under international law. States could assume Jurisdiction over Cyber-infrastructure and other activities based on it, including the Power to decide whether an act committed through it is lawful and enforce regulatory rules.

---

[101] Ibid
[102] Ibid
[103] M N. Schmitt (2014), *The Law of Cyber Warfare: Quo Vadis?* Stanford Law & Policy Review. Volume 25, issue 269, page 271
[104] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc A/68/98 paras 19–20.
[105] Ibid

3.2.2. Transnational Cybercrime and Territoriality Principle

The territoriality principle of international criminal Jurisdiction could be applied to transnational Cybercrime based on the following criteria. First, when the conduct is partly or substantial, it occurs within its territory. Second, if the subject cyber-infrastructure within its territory was involved in committing the act. Third, if the act has effects outside or is intended to have a substantial effect within its territory.[106]Therefore, factors such as the location of the act, person, effects, and the Computer System determine the applicability of the Territoriality Principle of Criminal Jurisdiction on transnational Cybercrimes.[107] The conduct which produced the effect did not take place within the territory. They allow States to deal with acts that originated within their territory and were completed abroad or act that originated abroad and were completed at least in part within its territory.[108]

As per the Convention on Cybercrime, in stipulating the applicability of the territoriality principle, States might assume Jurisdiction on the offense committed in a Nation's territory if the Convention covers it.[109]In the case of LICRA v. Yahoo regarding web pages showing Nazi memorabilia, material that is illegal to view in France is legal in many jurisdictions. Despite this, the French court assumes Jurisdiction over Yahoo and orders the removal of the webpage.[110]

There are two theories regarding applying the territorial principle on transnational Cybercrime based on the place and effects in the commission of Cybercrime. These two theories are called the Theory of uploader and downloader, depending on two distinct actors in Cyberspace.[111] The uploaders represent those who input Information into a site in Cyberspace, and the downloader who access it later without or with the intention of such exchanges and accessed by thousands of people worldwide.[112]

States could assume Jurisdiction based on the location where the Crime is presumed to be committed, which is the place the content is uploaded and the effect of the criminal act, i.e., downloaded on the abovementioned

---

[106] Wang, Kang-Kwong. *Transnational Cybercrime and the Territoriality Principle*. Journal of International Banking Law and Regulation, vol. 23, 2008, page. 657.
[107] Ibid
[108] Yahoo! France and Yahoo! Inc. v. License (Tribunal de Grande Instance, 24th Ch., Judges Mareille Déchamps, Christine Bitquenne-Leroy, André Delattre, Jean-Noël Gombaud, Arnaud Gilluin, Françoise Bairin Courbet & Jean-Daniel Politi), No. 2001/10455 (February 20, 2002).
[109] Elissa A. Okoniewski (2002), *Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet*, American University International Law Review Volume 18 | Issue 1 Article 6, page 297.
[110] Ibid
[111] Ikenga K. E. Oraegbunam (2016), *Towards containing the jurisdictional problems in Prosecuting cybercrimes: case reviews and responses*, NAUJILJ, volume 7, page 28.
[112]Ibid

case. The application of the territorial principle concerning Cybercrime raises a controversy concerning whether the location of Cybercrime is the place of downloading and uploading. American Online Service Provider, i.e., Yahoo in France was alleged to show *Nazi propaganda* and objects available for purchase on the French website, which was illegal in France.[113]

Even though the data could be uploaded from outside France and stored in *Yahoo* servers in the USA, the court asserted its Jurisdiction over *Yahoo*. Since the memorabilia and objects were available to residents located in France. Consequently, the tribunal ordered Yahoo to remove such content and destroy all the concerned files stored on its server. Therefore, this court considered where the data is downloaded as the base for exercising the territorial Jurisdiction over the Crime.[114]

Similarly, the special Statute of Computer Crimes in North Carolina states in the USA provides that the State will have Jurisdiction when the Crime committed using electronic communication may be deemed to have been committed where the electronic communication was originally sent or where it was initially received in the State which represents the place of uploading and downloading respectively.[115] Furthermore, it criminalizes fraud and related activity against protected Computers and includes Computers used in or affecting foreign commerce or communication, including Computers located outside the United States.[116]

3.2.2.1. Subjective Territoriality Principle and Transnational Cybercrime

This principle provides that a State assumes Jurisdiction over a criminal act if it can prove that the offender was in the territory of the State while executing the act. However, it might be irrelevant to the geographical location of the crime effect so far as it could be linked to the offender's activities. It also provides an essential framework for international law enforcement agencies to investigate and prosecute transnational Cybercrime.[117]

---

[113] Cedric Ryngaert (2015), *Jurisdiction in International Law*, 2nd Edition, Oxford University Press, Pro Catherine Redgwell and et eds, page 85
[114] Ibid n 87
[115]General Statutes of North Carolina, Section 14-453. Computer crime available on https://ncpro.sog.unc.edu/manual/101-1 accessed 01 December 2022
[116] Ibid
[117] Baker, A., & Chen, K.-H. (2013). *Transnational Cyber Crime and the Subjective Territoriality Principle*. International Criminal Justice Review, 23(1), page 30.

In 2017, the British authorities applied Subjective territoriality when arresting Lauri Love for alleged involvement in online systems intrusions against US networks between 2012 and 2013. [118]In 2018, German police arrested a Russian citizen known as Stanislav Lisov on cyber extortion and fraud charges. In this case, many of his victims lived outside Germany, and no evidence of Lisov's physical presence in Germany was available then. Then, Prosecutors were able to link him with Germany through accusations. He had used German services and Banking Institutions in committing his offenses.[119]

Additionally, Subjective territoriality also enables States to exercise Jurisdiction over Corporations whose businesses influence across borders but may not have distinct physical locations or present overseas operatives or agents within those Countries.[120]

There are four significant approaches concerning applying the territoriality principle on transnational Cybercrime and identifying the location of the commission of the Crime. The first approach is based on the location of the internet viewer/end-user, and the States concerned will have Jurisdiction over the act. Since the content or effect of the act could be visible anywhere or any place in which the content is available, it assumes to have the most logical solution.[121]

The second approach is based *on the location of the author, creator, or the most significant number of website creators as* the proper location to apply subjective territoriality. However, these approaches tend to promote impunity by the perpetrator of the act by simply evading themselves in one Jurisdiction in which the act is not criminalized though the effect of the act being laid on another State which criminalizes the act. [122]

A third approach is based on the *server's location o*n which the website or posting messages on the Internet requires storing or, at a minimum, transferring the Information through a central server. The notion that the location of the server can serve as the location of Jurisdiction may be easily detected. Despite this, the server's

[118] United States Attorney's Office, Southern District of New York, U.S. v. Lauri Love, S2 13 Cr. 367 (LAK) (Indictment), 15 July 2013.
[119]*Stanislav Lisov Guilty of Cybercrime in Europe,* Cyber Defense Magazine, May 17, 2019, available at https://www.cyberdefensemagazine.com/stanislav-lisov-guilty-of-cybercrime-in-europe/. Accessed on 20 December 2022.
[120] Singh, P. (2019). *Subjective Territoriality: Negotiating Meaning, Rules, and Order in the Low-Income City*. Singapore Journal of Tropical Geography, 40(2), page 153.
[121] Ibid
[122] Ibid

location may be detected by using phone networks to send Information through multiple States and several sub-servers, creating the additional problem of determining the primary server.[123]

The last and fourth approach considers the location where the website was first situated. Moreover, a website address begins as an Internet protocol (IP) address analogous to a street, and it can then be translated by one of several private registrars into an easy-to-use domain name. Though it may provide proof of location, it only partially solves the problem of territorial location based on IP addresses or domain names. Since these domain name suffixes are reserved for citizens of the countries, they indicate some technological development as VPN (Virtual Private Network) which could be used to trick such indications.[124]

3.2.2.2 Objective Territoriality Principle and Transnational Cybercrime

This principle applies to transnational Cybercrime in Countries that have the right to enforce their laws regulating Criminal activity occurring on the Internet, such as hacking and data theft when those crimes affect those who reside in or have a computer in the Country.[125]

A recent example is the French prosecutor's charge against the social media platform *Facebook* for failing to remove hate speech content from its platforms. Even though its primary headquarters were set up in California, USA, it had no substantial operations on French soil. The platform also argued that only US courts should apply here. Since France had no jurisdiction over them due to their lack of physical presence in France, the court proceedings were eventually undertaken according to French Jurisdiction using Objective Territoriality Principles.[126]

For this principle to be effective in transnational Cybercrime cases, all States involved must cooperate on an international level and recognize the legitimacy of other countries laws and judicial proceedings. States should coordinate their responses to these crimes through forums such as the Council of Europe's Cybercrime Convention and the International Network Against Cybercrime (INAC). In addition, States need to enforce

---

[123] Rozeman, C. (2015). *Application of the Principle of Subjective Territoriality in the Fight against Transnational Cybercrime*. Journal of International Criminal Justice, 13(3), page 558.
[124] Ibid
[125] Plattner, M., Bürger, D., Reichel, P., & Schwald, S. (2013), *Transnational crimes in Cyberspace and the principle of territoriality*. Computer Law & Security Review, 29(3), page 344.
[126] Paris prosecutor's office charges Facebook for 'failing to remove criminal hate speech content' from its platform." The Guardian. Guardian News and Media, 24 Jan. 2021, available on www.theguardian.com/technology/2021/jan/24/paris-prosecutors-office-charges-facebook-for-failing-to-remove-criminal-hate-speech-content/. Accessed on 01 January 2022.

laws that protect individuals from malicious acts committed via the Internet and ensure criminal liability extends beyond just perpetrators but also those who commissioned or sponsored illegal activities.[127]

This principle applies to traditional forms of Crime and Cybercrime, which has become increasingly enforceable across borders due to its global nature. The US has begun to recognize the need for international collaboration and has taken steps towards applying the territoriality principle about transnational Cybercrimes by signing bilateral agreements with other countries and joining intergovernmental organizations promoting cross-border Cooperation on cybercrime cases. [128] In 2020, the US joined the Council for Global Cooperation on Cyber Security (GCCS), an organization dedicated to working together to combat digital threats from all sources.

Additionally, through mutual legal assistance treaties (MLATs), the US can access Information related to potential criminal activity originating in another Country, aiding investigations into transnational cybercrime incidents. By being diligent Members of various Intergovernmental Organizations while holding up their end of these bilateral commitments, the US is demonstrating its commitment to upholding the territoriality principle and taking severe measures against transnational Cybercrime within its Jurisdiction.[129]

Among other things, the following approaches could be in place in applying the Objective Territoriality Principle to determine the jurisdictional Power of each relevant Nation. The first one is assessing an offender's connection to a particular Country or/and Nation that can determine which legal system they should apply to prosecute cybercrime cases that cross international borders. The second approach is implementing regional Cybercrime initiatives and increasing international collaboration among law enforcement professionals who are better equipped to investigate transnational cases under the objective territoriality principle and to develop more robust bilateral legal frameworks and specifically designed treaties for combating transnational digital Crime, incorporating guidelines on how objective territoriality applies in Cyberspace. [130] The third one is establishing a joint venture with specialists from different

[127] Ibid 117
[128] Teske, D., Lindblom, J., & Harrington, C. (2018). *Objective territoriality in transnational Cybercrime: Practical cases from the United States*. International Journal of Cyber Criminology, 12(2), page 102.
[129] Ibid
[130] Guske, I., Oh, N.-K., & Urban, L. (2008). *Applying 'Objective' Territoriality Principle: Analysis of Transnational Cybercrime Case in International Law*. Journal of Computer and Law, 21(4), page 287.

Countries for close technical Cooperation and sharing resources for investigations into complex crimes that cross multiple National Jurisdictions.[131]

In 1997, Germany also passed the Information and Communications Services Act, establishing a conduit liability for Internet service providers (ISPs). Under the Act, ISPs had a duty to block and make unavailable materials found to be illegal under the Act, when they knew the illegal material existed; failure to remove or block the material after it was discovered would result in criminal prosecution.[132]

Since the act was committed within the territory and the other based on the effect of the criminal act laid on the specific territory, there might be a situation in which two or more States claim Jurisdiction on one specific Crime due to overlapping in the Jurisdiction between States. Accordingly, to identify the appropriate Jurisdiction on transnational Crime, there are a wide range of factors inter alia locus of the accused and acts, where the effect or result of the act has occurred, the scale or degree of harm done, the intention of the accused, nationality, and domicile.[133]

The tests used to determine the appropriate Jurisdiction to adjudicate the case of transnational nature illustrated are the *Minimum Contacts Test, Purposeful Availment Test, Effects Test, and Sliding Scale Test*. The tests were developed to claim Personal Jurisdiction on Crime and civil cases with extra-contractual nature. They could also be applied to assess the applicability of the territoriality principle on transnational Cybercrime. Since personal Jurisdiction interjects with the territoriality principle in such a way, states assert Jurisdiction by the fact that the perpetrator of the Crime committed the act within the territory of the State or the effect of the act has an impact on the State's territory. Most notably, in one way or another, they must include the criterion made to identify the appropriateness of Jurisdiction.[134]

3.2.3. Minimum Contacts Test

The United States Supreme Court establishes this principle of minimum contact and is commonly used in deciding the Jurisdiction of the Court. It elaborates that there needs to the existence of some minimal contact between the accused and the Court to meet the requirements of due process provisions and fairness.[135]

---

[131] Ibid
[132] German Information and Communications Services Act (IuKDG), 1997, Bundesgesetzblatt Teil I, Nr. 57/1997.
[133] Satwinder Kaur (2013), *Determining Jurisdiction of Cyber Crimes: Challenges and Issues*, International Journal of Research in Engineering and Technology, vol 2, page 13.
[134] Ibid
[135] Lan, Guobin & Ling, Polun. (2007). *Transnational Cybercrime and Territoriality Principle: An Analysis of Minimum Contacts Test Regarding Extraterritorial Heat in Cyberspace*. International Journal of Cyber Criminology, 1(1), 180-198.

According to the principle of minimum contact, establishing the relationship of Jurisdiction between the perpetrator and the Court requires minimal contact. This criterion of minimum contact could be elaborated that the Courts may exercise Jurisdiction over unlawful acts if the perpetrator intended to be protected by the laws of other States or if he proactively places his network activity under the Jurisdiction of other State Courts.[136] Furthermore, If the perpetrator simply provides unilateral Information on the site and does not interact with the State claiming Jurisdiction, the Court should not exercise Jurisdiction. However, Courts may be able to exercise jurisdiction over transnational Cybercrime. If the perpetrator, in addition to providing information, offers other related services or online transactions of the goods when interacting with visitors within the territory.[137]

Courts may exercise general Jurisdiction over a non-resident only if the perpetrator is physically present in the forum State or maintains continuous and systematic contact with that forum State. However, the court will have Jurisdiction if the act is committed within the territorial Jurisdiction of the Court. Consequently, it will be assumed to have complied with the traditional notions of fair play and substantial justice. Among other things, the tests consider the burden placed on the defendant, the forum State's interest in the outcome, the plaintiffs' interests in obtaining relief, the judicial system's interest in a most efficient resolution, and furthering social policies shared by the States. [138]

In the UK, the core statute is the Computer Misuse Act 1990 provides the concepts of a significant link to claim Jurisdiction over offenses involving unauthorized access to computer material. In addition, Section 5 refers to the criteria, including the accused's nationality, the presence of affected computers within the UK, and a significant risk of damage to human welfare, the environment, the economy, and national security.[139]

3.2.4. Purposeful Availment Test

It is a legal concept used to determine whether a perpetrator of the Crime had sufficient jurisdictional contact with a specific State when the alleged offense occurred in that State or not. Moreover, it is relevant to

---

[136] Ibid

[137] Macfarlane, E. (2020). *The Transnational Cybercrime and Territoriality Principle: A Minimum Contacts Test.*, available on https://cyberlawclinic.blog/2020/08/11/the-transnational-cybercrime-and-territoriality-principle-a-minimum-contacts-test/accessed on 01 January 2022.

[138] Ibid

[139]Computer Misuse Act 1990 UK legislation, The National Archives. Available on https://www.legislation.gov.uk/ukpga/1990/18/contents accessed 02 January 2022.

transnational Cybercrime to decide concerning the criminality of acts committed across national borders. It is subject to the same territoriality principle used by the prosecution in cases of physical crimes.[140]

In evaluating Purposeful availment, Courts will consider whether the perpetrator's act was related to criminal activities intentionally directed towards the forum State and applicable laws. For example, if the perpetrator knowingly accessed distant servers located within a particular State to commit data theft or other computer-related crimes, this evidence could be used to demonstrate Purposeful availment. Additionally, if the perpetrator knew that by engaging in their criminal activities, they would incur consequences in the forum State, such as reputational damage or civil liability for damages caused by their breach of duty or commission of an unlawful act. It could also be considered evidence of purposeful availment.[141]

In the United States v. Aleksei Burkov case, Burkov was a Russian national who operated a website that facilitated illegal activities such as credit card fraud, identity theft, and drug trafficking. The website was accessible to users in several countries, including the United States. He also used servers in the United States to carry out his illegal activities. Burkov was eventually apprehended by Israeli authorities and extradited to the United States to face charges.[142]

In this case, purposeful availment tests would have been used to determine whether Burkov had deliberately targeted users in the United States through his website and had intentionally availed himself of United States laws by using servers within the Country.[143]

The purposeful availment doctrine determines whether a defendant has purposefully availed themselves of the benefits and protections of a particular jurisdiction's laws and legal system. This test is often used in cases involving transnational Cybercrime where the offenders use the Internet to commit illegal activities across multiple countries. This illustrates how Courts are attempting to overcome the challenges associated with transnational Cybercrime while retaining the application of territoriality principles such as international comity where one State respects another involved States laws and Jurisdiction following consideration of

[140] Thomson, D. (2006). Global Constitutionalism: Cyber Crimes, Territorial Sovereignty, and International Conflict? University Of Toronto Law Journal, 56(1), 75-119. https://www.utlj.org/content/global-constitutionalism-cyber-crimes-territorial-sovereignty-andinternational-conflict
[141] Ibid
[142] United States v. Aleksei Burkov, 1:15-cr-00245-TSE,2020
[143] Ibid

Sovereign interest and relevant conflicts with both attorneys using the concise reference to applicable legal authorities defining violations present in this case.[144]

Furthermore, to determine if the Purposeful Availment Test applies to transnational Cybercrime and the territoriality principle, one must examine both elements of this legal standard, whether *"purposeful direct activities"* have been taken about an Individual or State and whether there are commercial advantages gained by transacting in that location due to lower costs, access to different customer profiles, strategic positioning, or other such factors. [145]

In general, Transnational Cybercrimes rely on some element or action that could be viewed as a purposeful direct activity for them to gain from their activity. Therefore, the Purposeful Availment Test can be applied to Transnational Cybercrimes and the territoriality principle. Indeed, proof of a deliberate aim to gain from Criminal behavior may help to support Criminal prosecutions on either side of National borders and existing enforcement efforts.[146]

3.2.5. Effects Test

The effects test on transnational Cybercrime with the territoriality principle can be significant regarding its implications for international law enforcement. It affects both the technical and legal aspects of global criminal regulation. When transnational crimes occur via Computer networks and other methods, it can be challenging to determine who should be held responsible since it could have multiple effects. [147]

From a technical side, it may not always be possible to trace an attack originating from another Country back to its source or its damages inflicted by a perpetrator living in yet another location. Law enforcement agencies will also struggle with identifying how to hold those perpetrators accountable when multiple jurisdictions are involved, as well as evidence gathering and prosecution issues. These challenges emphasize the need for enhanced E-Crime prevention and investigation means on an international level and improved Cooperation between Countries to mitigate this best increasingly global phenomenon.[148].

---

[144] Baglesman, Robert. (2014). *Hot Spots, Cool Responses: Transnational Cyber Crime and the Territoriality Principle.* Northwestern University Law Review, 108(3), page 1035.
[145] Ibid
[146] Ibid
[147] Verdi, E., & de Hert, P. (2018). *The effects test Applying the territoriality principle of international law to transnational Cybercrime*—International Review of Law, Computers & Technology, 32(3), page 277.
[148] Ibid

The effect test for determining the territoriality principle on transnational Cybercrime involves considering how much of a tangible effect a Crime has within one Jurisdiction compared to other jurisdictions. When most effects occur in one Jurisdiction, that Jurisdiction should have greater authority to take action against the perpetrator. This will allow for more local accountability and protection for victimized individuals. Additionally, if a crime is sufficiently connected to multiple jurisdictions, for example, by utilizing the communications infrastructure or networks located within those jurisdictions, all affected Countries could hold someone responsible depending on the nature and scope of the Crime.[149]

In the case of Calder *v. Jones*, a US Supreme Court case that involves claims of libel, invasion of privacy, and intentional infliction of emotional harm through an article on October 9, 1979, that appeared in the National Enquirer about the respondent, Shirley Jones, who was an actress and the defendant. In the article, the editor-in-chief alleged that Jones was an alcoholic. The California Court explained that having Jurisdiction based on effects test based on intentional aiming of harmful conduct at a forum State and causes harm the perpetrator knew was likely to be suffered in the forum State.[150]

3.2.6 Sliding Scale Test

This test considers various factors that could influence the interpretation of territoriality in each case, such as the location of the offender, the State where the Crime was committed, the seriousness of the offense, and whether a particular Country has an interest in punishing an offender or protecting its Citizens from future Cybercrime activities.[151]

It would weigh on how legally binding decisions are made across different Nations and Regions, as well as any overlapping authority between those regions. The concept could also be applied to determine if specific laws should take precedence over others and conditions to do so. Besides, where multiple systems of legal regulation operate concurrently in a shared space/territory, the test can help identify power-sharing arrangements and determine which parts of each system should have priority over another.[152]

---

[149] Ibid
[150] Calder v. Jones, 465 U.S. 783 (1984).
[151] Handelman, D. (2004). *The Sliding Scale of Test Transnational and Territoriality Principle*. In K. W. Weiler & J. Gilliom (Eds.), *International human rights law: Philosophical perspectives* Oxford: Oxford University Press. Page 365.
[152] Barker, J. (2018). *Modern Territorialism: Exploring the Role of Territoriality Principle in Transnational Cyber Crime Cases*. International Law Studies, 94(284), page 230.

The sliding Scale Test requires carefully evaluating all relevant facts to determine where a particular case should be tried, on the specific forum, and which laws should be applied.[153]The test was developed in the case of Zippo Mfg. Co. v. Zippo Dot Coin, in which the court holds that Pennsylvania state has Jurisdiction over California Internet news provider because of the defendant's contracts with 7(Seven) Pennsylvania Internet service providers and with 3000 Pennsylvania residents.[154]In this case, the Court considers whether the website viewers have a way to respond and whether the website is an integral part of the defendant's business. Since it shows the connection of the concerned forum with the actor of the criminal act, it was considered as the harm of the act on the forum State.[155]

3.3. Application of Territoriality Principle on Transnational Cybercrimes

To assess the applicability of the principle of territoriality on transnational Cybercrime, we have discussed the background of the principle based on the authority that emanates from the Sovereignty of States to maintain law and order within the territoriality and the transnational Cybercrime committed through Cyberspace which contested to be out of the Sovereign Power of States.

Despite the contention about whether Cyberspace could be under the purview of States' Sovereignty or not, Customary international law was/is developed for the regulation of Cyberspace and transnational Cybercrime by linking the technology with State's territory and considering the facts that Crime could result from damage to peace and tranquility.

The territoriality principle of international criminal could apply to subjective and objective principles of transnational Cybercrime when it is committed within the territory of the States and the effect/consequence of the crime results in the territoriality of the State regardless of the nationality of the perpetrator of the Crime respectively. Both principles are essential in determining the Jurisdiction of crimes in international law and can be used to ensure that justice is served.

The assumption of Jurisdiction based on territoriality principles has never been easier in transnational Cybercrime. Hence, the nature of the technology allows Crime to be borderless, and it could also be committed from anywhere in the globe and have effect anywhere. Thus, more than one State could assume Jurisdiction over a single transnational Cybercrime.

---

[153] Ibid
[154] Zippo Mfg. Co. v. Zippo Dot Coin, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997)
[155] Ibid

Due to this reason, while assuming Jurisdiction based on the territoriality principle, there could be more than one State's claims to assume Jurisdiction. To get some clarity on deciding the most relevant and appropriate Jurisdiction to regulate transnational Cybercrime, there are tests developed through time that could help us to determine the most appropriate jurisdictions. They prioritize one criterion as a base for assuming Jurisdiction by the State/ Court over the other. The minimum contact test proposed that the contract which the Court has with the perpetrator or the alleged actor in the commission of the act of Cybercrime could be taken into consideration while deciding the relevant and appropriate Jurisdiction. Besides, this test checks the fairness and justice to be served by the exercise of this Jurisdiction.[156] On the other hand, the Purposeful availment proposed that the person's intention to avail himself for the specific territory of Sovereign States could be considered as one factor in assuming Jurisdiction over the criminal act. In this sense, if the perpetrator intentionally connects himself while executing the act, the States within that territory should have Jurisdiction to adjudicate the case.[157]

Apart from the two tests which focus on the relationship between the states and the perpetrator of the Crime. The effect tests focus more on the consequence of the criminal act by the perpetrator of the transnational Cybercrime. Thus, this test prioritizes the assumption of Jurisdiction by the State in which the act's effect has occurred. Moreover, when the damage /consequence of the act is made on the multiple States, it proposed that the States which have significant links or are significantly affected by the act could assume Jurisdiction. By emphasizing the act's effect, this test considers being more favorable for applying the objective sense of territoriality principle.[158]

In the case of Blakey v. Continental Airlines, the employee made an allegation concerning whether an employer must be held liable for harassment that could occur on an internal internet bulletin board. Since both the effect on the forum and the defendant's contact with the forum were considered, the minimum contacts test has been applied along with the effects test to assess the Court having proper Jurisdiction.[159]Here, two or more tests could resolve complications in deciding the appropriate Jurisdiction.

---

[156] Ashabari Basu Thakur, *Determination of Jurisdiction in Cyber - Crimes: Issues and Challenges available on https://www.legalpedia.co.in/articlecontent/determination-of-jurisdiction-in-cyber-crimes-issues-and-challenges.html accessible on 23 March 2023.*

[157] Ibid

[158] Saloni Khanderia(2020), The curious case of personal Jurisdiction for cyber-based transnational transactions in India: Does one size fit all? Available at https://conflictoflaws.net/2020/the-curious-case-of-personal-jurisdiction-for-cyber-based-transnational-transactions-in-india-does-one-size-fit-all/ accessed on 02 May 2023.

[159] Blakey v. Continental Airlines, Inc., 992 F. Supp. 731 (D.N.J. 1998)

Lastly, the sliding scale test proposes that all relevant facts connected and related to the State's Jurisdiction should be considered rather than giving one factor over the other. The decision considers the specific contexts of each case and each factor that affects the case, making it a more holistic approach to resolving possible jurisdictional overlapping.

To sum up, despite the existence of testes developed to resolve the possible conflict of jurisdiction the international laws on cybercrime has not provide clear guideline to resolve the problem by applying tests/parameters used to assume jurisdiction. Furthermore, there are other challenges which emanates from the special nature of the crime being transnational and committed in Cyberspace.

Chapter Four

Challenges in Applying Territoriality Principle of International Criminal Jurisdiction on Transnational Cybercrime

Having seen the applicability of the territorial principle of International Criminal Jurisdiction on transnational Cybercrime and tests that could be used while deciding the specific application of the principle. This chapter will discuss the challenges faced while applying the territoriality principle of criminal Jurisdiction to transnational Cybercrime.

Transnational cybercrime involves criminals who deliberately fashion their attacks to exploit the potential weaknesses present in the ICT infrastructures with transnational nature. On the other hand, there is a worldwide target pool of computers and users to victimize or exploit in denial of service or other attacks. This will enable attackers to do more damage without effort than attacking computers or users in a single State. Furthermore, disparities among States in the legal, regulatory, or policy environment concerning cybercrime will give extra support to the perpetrators of the crimes on their way to impunity.[160]

Among other things, lack of international cooperation, lack of unified and accepted laws governing cyberspace, and Unclear legal authority over foreign nationals could be significant challenges in applying the territoriality principle of criminal Jurisdiction on transnational Cybercrime, and these points will be discussed in the following Sections of the Chapter.

4.1. Lack of International Cooperation

The principle of cooperation between States is accepted as a Preemptory norm set forth by international documents, including the United Nations Charter, the Vienna Convention on the Law of Treaties, and other critical international documents.[161]On the other hand, the territoriality principle is a fundamental principle of international law that a Sovereign State has the exclusive right to exercise Jurisdiction within its territory. However, applying the territoriality principle to transnational cybercrimes can be challenging because of its borderless nature.[162]

---

[160] Toni M. Mastrobueni, Sally MacIntyre(2016), *Cybercrime Law and the International Framework: A Transnational Analysis,* ICMCP Journal of Cybersecurity & Privacy, page 23.
[161]Ibid
[162] Ibid

Effective implementation of the territoriality principle on transnational Cybercrime enshrined under international agreements depends on the cooperation between States concerned. Otherwise, more than merely agreements between states might be required to respond to transnational cybercrimes effectively.[163]

Besides, States might refrain from participating in international legal initiatives or joining relevant conventions to strengthen global efforts against organized crime and transnational Cybercrime for different reasons. States may need help to provide adequate assistance with each other's investigations or prosecution. [164] Thus, ensuring the prosecution of the perpetrator requires greater collaboration between States through joint agreements over sharing evidence from cybercrimes conducted in different Countries.[165]

To this effect, international cooperation is essential in applying the territoriality principle to transnational Cybercrime inter alia involves cooperation between law enforcement agencies. Hence, applying the territoriality principle to transnational Cybercrime requires a complex and multifaceted approach that involves cooperation and coordination between states and international organizations.[166]

The case regarding the attack of WannaCry, a malware that encrypts files on infected systems, demanding payment in exchange for decryption in 2017, could be mentioned. The act affected several computer systems across 150 Countries, including the UK's National Health Service, forcing hospitals to cancel surgeries and appointments.[167] Even though North Korea was accused of being responsible for the attack, it was difficult to prosecute the perpetrators due to a lack of cooperation from other Countries and challenges in tracking down the individuals involved.[168]

Another exemplary case is related to the Syrian Electronic Army (SEA)[169] Which is a group of hackers who support the government of Syria in its conflict with other Countries. It was responsible for a series of attacks on U.S. government websites and French and Israeli government websites from 2011 to 2015. However, any

---

[163] Holt, T.J., Simons, W., Kalra, A., King, P. and Zhang, H. (2016). Effective Implementation of the Territoriality Principle: Responding to Transnational Cybercrime. Journal of International Criminal Justice, 14(3), page 615.

[164] Lei, Dong-hoon Thomas (2017), *Intergovernmental Cooperation in Transnational Cybercrime Investigations: Exploring Challenge*s, Third World Quarterly, Vol. 38 Issue 9, page 1710.

[165] Ibid

[166] Ibid

[167]Cyber-attack: US and UK blame North Korea for WannaCry, available on https://www.bbc.com/news/world-us-canada-42407488 accessed on 23 April 2023

[168]Ibid

[169] *The Syrian Electronic Army (SEA) is a hacktivist group responsible for numerous cyber-attacks since 2011. The group has targeted websites associated with governments, media organizations, and political groups, such as the BBC, The Guardian, and Forbes. The SEA also attempted to hack into several presidential campaigns during the 2012 US election cycle*. (See Yen, C. (2014). *How the Syrian Electronic Army is shaping international politics*. Journal of Contemporary Studies, 3(2), 37-45.)

country has ever successfully prosecuted the Syrian Electronic Army. Lack of cooperation has allowed the Syrian Electronic Army to remain unpunished and impunity to continue to be a problem in transnational Cybercrime.[170]Later, only Peter Romar, a Syrian Electronic Army member, was extradited from Germany to the United States on May 10, 2016, to face charges brought by the Department of Justice for engaging in a criminal conspiracy against U.S. entities by conducting Computer intrusions.[171]

To sum up, applying the territoriality principle of criminal Jurisdiction in prosecuting cases of transnational Cybercrimes requires the Cooperation of States. Despite this, many States are unwilling or unable to cooperate on matters related to transnational Cybercrime effectively due to geopolitical considerations. In addition, the Lack of cross-border collaboration makes it extremely difficult for investigators and prosecutors from different Countries to work together on cases involving complex crimes committed in Cyberspace.

4.3. Lack of unified and accepted laws governing cyberspace

Considering the problems posed by transnational Cybercrime, States have adopted legislation and international instruments to regulate and prosecute the perpetrator of Cybercrimes. However, this effort by the States is only made with challenges. Among the challenges, the lack of unified and accepted laws in applying territoriality criminal jurisdiction on transnational cybercrime could be one. Since no single governing body sets out unified laws related to digital crimes, there are no universal and widely accepted standards to address complex cyber issues. It makes it difficult for Countries to intervene and act against malicious online activities.[172]

Additionally, legislation regulating transnational Cybercrime varies from Country to Country due to differences in culture, resources, levels of development, and technical capabilities.[173] Thus, taking on transnational Cybercrime can be complicated and lengthy as each Nation must draft its legal systems and procedures for dealing with such threats before being able to cooperate with others.[174]

---

[170] Ibid

[171] Nakashima, Ellen (2016). *"Syrian hacker extradited to the United States from Germany* ."Washington Post Available on https://www.washingtonpost.com/world/national-security/syrian-hacker-extradited-to-the-unitedstatesfromgermany accessed on 01 January 2023.

[172] McCarthy, B. (2019). *Transnational Cybercrime: Challenges in Establishing Territoriality in Criminal Jurisdiction*. International Criminal Law Review, 19(4), 514.

[173] Asphyxia Webb(2014), *International Efforts to Combat Transnational Cybercrime,* Available at: http://lawthinktank.weebly.com/international-efforts-to-combat-transnational-cybercrime--an-overview.html accessed on 13 January 2023.

[174]Ibid

The assumption of Jurisdiction on transnational Cybercrime does not only require a connection with the crime or the perpetrator. It also demands that this connection be sufficiently close to warrant the exercise of Jurisdiction. Various jurisdiction clauses result in positive or negative jurisdiction conflicts when multiple States claim Jurisdiction and no State claims Jurisdiction on the presumption, respectively.[175]

In this regard, the well-known case relating to the "I Love You" virus in 2000 from the Philippines caused up to $10 billion, which the U.S. Investigators pressed to have the suspects in the attack Computer programming students from the Philippines arrested and prosecuted.[176]Despite the investigators attempting to prosecute the perpetrators, as per the 1998 law prohibiting the use of access devices. Chief State Counsel concluded that the law could not be used. Since '*the intention of a computer hacker is not to defraud but to destroy files*.' Moreover, the Philippines had no ICTs laws, so creating and disseminating a virus was not a crime.[177]

Therefore, the law enforcement officers had a hard time convincing a magistrate to issue a warrant to search the suspect's apartment. Later, the suspected virus author could not be prosecuted under the repertoire of offenses defined by the Philippines criminal code.[178] Afterward, the Philippines adopted a law punishing those who spread computer viruses with up to three years imprisonment and fines from $2,350 to a maximum for the damage caused. However, the new law will not apply retroactively. This costly act has gone unpunished.[179]

Due to these challenges, an international organization's efforts have achieved worldwide attention to the problem of transnational Cybercrime and promoted international harmonization of legal approaches. The national efforts to combat Cybercrime present in States are at different levels of sophistication and priority.

---

[175] Peerenboom, R.P(2014), *Business and human rights: implications of jurisdictional regimes for economic activities with a transnational dimension*. Comp. J Int'l & Com L. 28, page 231.
[176] Alan Elsner (2000), *Virus Attack Causes Billions in Damage,"* Reuters, May 15, 2000. Available on https://www.reuters.com/article/us-virus-attack-costs/virus-attack-causes-billions-in-damage-idUSL15116450 accessed on 16 January 2023
[177] Ibid
[178] Gahutan, M. (2009). *The Anti-Virus Law of the Philippines. Malaya Business Insight*, Accessed on 11 February 2010 from www.malaya.com.ph/apr14/tech1.html on 18 January 2023.
[179] Ibid

[180]However, the main problem in writing, enforcing, prosecuting, and interpreting cybercrime laws is a need for more technical knowledge about Cyberspace and technology.[181]

4.4. Unclear legal authority over foreign nationals

The territoriality principle dictates that States may only exercise authority within their borders, creating a challenge when dealing with transnational Cybercrime in the following scenarios. First, when a foreign national is convicted of a cybercrime in one Country, the conviction does not have apparent legal authority over the foreign national in the other Country where the Cybercrime was committed.[182] Second, when a foreign national is alleged to have committed a Cybercrime in one Country, there is no apparent legal authority over the foreign national in the other Country where the Cybercrime was committed. Moreover, third, when the computer systems of a foreign national are allegedly used to commit a cybercrime in one Country. However, there is no legal authority over the foreign national in the other Country where the Cybercrime was committed.[183]

If the involved Countries do not have an extradition treaty, obtaining evidence from foreign entities can be difficult. Additionally, due to the complexities in tracing digital activities and communications, there can be delays or breakdowns in communication between different global authorities. Furthermore, Countries have different technological capabilities, such as access to sophisticated software programs needed for comprehensive forensic analysis. All this can complicate when applying territoriality principles to transnational Cybercrime.[184]

Applying the territoriality principle on transnational Cybercrime, the unclarity regarding authority or Jurisdiction over foreign nationals can be mentioned. Countries have laws protecting their Citizens from Cybercrimes but little legal authority over foreigners committing such acts outside their territories.[185] Despite the States becoming increasingly interconnected, internationally agreed-upon frameworks or standards for

---

[180] Smith, L.P. (2018). *The Fight Against Transnational Cybercrime: International and National Efforts*. Santa Clara Computer & High Technology Law Journal, 34(2), page 524.
[181] Ibid
[182] Jared A. Deifik & Bryan S. Turner (2015), *Applying Territoriality Principles to Transnational Cyber Crime: A Proposal for International Legal Harmonization*, 39 Vermont Law Review, page 515.
[183] Devlin Balko (2018), *State or Nation? Assessing Jurisdiction Over Transnational Cybercrime*, Brigham Young University Law Review, page 233.
[184]Sigler, Anja E. (2018), *Implementing Intergovernmental Cooperation for Cyber Crime Investigations: The Significance of Territoriality*, European Journal of Enforcement, vol. 6, no. 2, page 212.
[185] Ibid

combatting transnational Cybercrime and upholding the territoriality principle still need to be improved. Thus, international cooperation and collaboration may be needed to address crimes across different jurisdictions and states effectively. Different across countries and with no precedence or understanding of international laws on Cybercrimes poses difficulty concerning condemning and convicting foreign nationals under domestic or supranational Courts.[186]

In the United States v. Nikulin case, a Russian national named Yevgeniy Nikulin was accused of hacking into several American websites, including LinkedIn and Dropbox, and stealing user data. Eventually extradited from the Czech Republic to the United States. The case raised questions about the legality of such extraditions in cases where the alleged crimes were committed outside of the United States and foreign nationals,[187] It also highlighted the challenges of prosecuting foreign nationals for Cybercrimes that cross international borders and involve multiple jurisdictions with different laws and regulations regarding Cybercrime. Furthermore, the complex legal landscape surrounds transnational Cybercrime and the challenges of prosecuting foreign nationals who commit these crimes across multiple jurisdictions.[188]

The challenge for law enforcement in this context is that there often needs to be apparent legal authority over foreign nationals who mainly reside outside the Forum State. In some cases, Cybercrime may be considered a violation of a foreign country's physical or cyber security. However, in other cases, it might be considered a violation of the privacy of a foreign individual.[189]

4.2. Determining the source and effect of the act

Applying the territoriality principle to transnational Cybercrime requires accurately determining where an alleged Cybercrime was committed. More specifically, the act's source and effect constitute the crime's element. On the other hand, transnational Cybercrimes may originate from one State, and their effect or damage can be felt in multiple Countries. Furthermore, due to the nature of the internet, it is sometimes difficult to precisely identify who is responsible for a crime or attack.[190]Therefore, in the case of transnational Cybercrime, determining the location of a crime based on geographical area is not easily possible as in

[186] Ibid
[187] United States v Nikulin, 2018 USDC NDCA 15-00249, United States District Court for the Northern District of California.
[188] Ibid
[189] Hoffman, Nuijten, M., & Ying, F. (2020). *Cybercrime: Cross-Border Cooperation and Extraterritorial Enforcement.* International Studies Quarterly, 64(3), page 121
[190] Moore, T.J., Anderson, R.B. & Parsons, C. (2011). *Cyber calcification: locating Cybercrime in a transnational law enforcement context*. International Journal of Law, crime, and Justice, 39(3), page 188.

traditional crimes because the non-material nature of Cyberspace and anonymity hide the perpetrators from detection.[191]

According to Johnson and Post, Cyberspace dramatically undermines the relationship between legally significant occurrences and physical places. They claim that the growth of the global Computer network is destroying the link between geographical location and the power of local governments to assert control over online behavior. Furthermore, they have concluded that Cyberspace hampers the rulemaking system based on borders between physical places, at least concerning the concept that territorially defined rules should naturally administer Cyberspace.[192]

For law enforcement officers, determining the source of an act or locating the perpetrator's place to identify where a transnational Cybercrime was committed could be difficult. Hence the perpetrator might also use multiple Computers located in various locations worldwide. This will make it more complicated to invoke the principle of territoriality in cases when the accused potentially have committed an offense in one or more jurisdictions unknown to law enforcement officers.[193]

Hence, these crimes involve cross-border Computer networks, and jurisdictional issues become complex as multiple States could potentially lay claim over the effects of an attack and attempt to prosecute suspects. This could lead to a conflict of interest between States and further complicates efforts at applying the territoriality principle to transnational Cybercrime.[194]

In the U.S. v Aleynikov, a case concerning alleged criminal copyright infringement in which high-frequency trader Sergey Aleynikov was accused of taking proprietary computer code from his employer, i.e., Goldman Sachs & Co Goldman Sachs & Co. The code was found to have been copied into his home computers and uploaded to overseas servers. Afterward, the Canadian government charged Aleynikov for his illegal activity, Since Company's servers were hosted by Canadian ISP providers whose connections passed through Canada's national borders into the US via Companies on grounds. Since it is transnational and takes place inside and outside America's border, both States intend to retain the power to prosecute.[195]

---

[191] Ibid
[192] Johnson, J.E., & Post, D.G. (2009). *Transnational Cybercrime: The Evolving Threat of the 21st Century*. The Howard Journal of Criminal Justice, 48(1), page 91.
[193] Ibid
[194] Griesser, D., Grünfeld, L., & Voigt, S. (2017). *The challenges of international cybercrime prosecution: Reflections on territoriality in a globalized world*. International Journal of Cyber Criminology, 11(2), page 35.
[195] United States v. Aleynikov, No. 11-1126 (2d Cir. 2012)

After considering these factors, the two States eventually agreed they would defer exercising their sovereign powers because Criminal laws could reasonably be interpreted within either State's jurisdiction basis and delay decision-making until a better solution arises. [196] However, after consideration of interstate comity between the two States, US Government refused requests by the Canadian prosecuting Attorney, who sought extradition proceedings against Aleynikov, which enabled United State Court to take over proceedings. Since the effect of the crime happens in both States and will result in overlapping Jurisdiction, determining the effect could be problematic.[197]

In another case, Roman Valeryevich Seleznev, a Russian citizen, was indicted on charges including hacking into point-of-sale systems and stealing credit card data from hundreds of businesses in the United States. The prosecution argued that Seleznev was the mastermind behind several criminal schemes that involved the sale of stolen data on underground online forums. [198] The government presented evidence that showed how Seleznev used various methods to gain unauthorized access to Computer systems, steal data, communicate with co-conspirators, and distribute the stolen data for profit. The jury found Seleznev guilty on multiple counts, including wire fraud, intentional damage to a protected computer, identity theft, and trafficking in unauthorized access devices.[199] This case highlighted the complex nature of transnational Cybercrime and the need for international cooperation to combat it. It also demonstrated how prosecutors could build a case to determine cause and effect in Cybercrime by presenting evidence that shows the defendant's involvement in the crime, his or her intent, and the effects of the crime on the victims.[200]

[196] Ibid
[197] Ibid
[198] United States v. Seleznev, 820 F.3d 1094 (9th Cir. 2016I)
[199] Ibid
[200]Ibid

Chapter Five

Conclusion and Recommendations

The territoriality principle of International Criminal Jurisdiction is a legal principle that States sovereignty to maintain law and order within the territory. Consequently, States have Jurisdiction over crimes committed within their territory. The principle has been used to prosecute individuals for computer network crimes. However, some scholars argue that the territoriality principle should not be applied when online crimes occur. Since there is no clear physical boundary between Countries in Cyberspace, it is beyond any State's sovereignty. On the other hand, some state that the principle should be applied with greater flexibility to account for the unique nature of Cybercrime. Thus, there is a need to assess the applicability of the territoriality principle to transnational Cybercrime and consider the challenges faced.

Various international instruments came into effect considering the challenges posed by transnational Cybercrime. Among them, Convention on Cybercrime (2001) and its additional protocols, the African Union Convention on Cybersecurity and Personal Data Protection, and Arab Convention on Combating Information Technology Offences were discussed, and each have significant value in the criminalization and prosecution of transnational Cybercrime from defining the act up to setting procedure for mutual assistance between State. It was also shown that our Country, Ethiopia has the Legal framework to apply the territoriality principle on transnational Cybercrime based on the Criminal Code and Computer Crime Proclamation. However, Ethiopia is not a signatory to any major international and regional instruments on Cybercrime.

The territoriality principle can apply to transnational Cybercrime with both Subjective and Objective territoriality ways. In case when an act that violates the law takes place within the territory of the forum State, then the forum State has the Jurisdiction to try the case with subjective principle, State is entitled to try criminals for offenses fully committed within its territory, provided that the act is commenced elsewhere but completed within another State territory with objective principle.

Due to the transnational nature of Cybercrime, the crime could have emanated from States which is different from the place of the effect of the criminal conduct and have effect in multiple States. Because of this prominent and other reasons, the assumption of territoriality jurisdiction on transnational Cybercrime was never more straightforward and needed applications of some tests to resolve such conflict and overlapping of Jurisdiction.

Different factors must be considered in determining the practical applicability of the territoriality principle of criminal Jurisdiction on transnational Cybercrime. Based on this, there are four illustrated tests or theories. The principle of minimum contact, which the United States Supreme Court established, depends on the existence of some minimal contact between the accused and the court to meet the requirements of due process provisions and fairness. On the other hand, Purposeful Availment tests provide that there should be sufficient jurisdictional contact with a specific State when the alleged offense occurred in that State.

Another two tests namely the effect and sliding scale test has been developed in resolving the conflict of jurisdiction. Based on the effect of the criminal act and considering various factors in prioritizing one parameter over the other respectively.

There have been several challenges to the applicability of the territoriality principle in the context of Cybercrime. The First challenge is that many cybercrimes are not necessarily perpetrated within the territory of a particular country. As a result, it may be difficult for Courts to determine which Country should have Jurisdiction over these offenses.

The second challenge is that cybercrimes involve multiple countries' citizens or residents. The Lack of cooperation between different jurisdictions and clarity regarding authority over foreign nationals accompanies this. This would challenge States to exercise Jurisdiction by applying the principle. Besides, the international and regional Conventions' failure to specify the priority to be given when there is a conflict of Jurisdiction between States poses significant challenges. Lastly, Cybercrime often takes place anonymously. To prove that a cybercrime is carried out to cause harm or damage, difficulty in identifying the perpetrator or victims of a cybercrime is another challenge in applying the territoriality principle to transnational Cybercrime.

Consequently, to avert the challenges and successfully apply the territoriality principles of criminal Jurisdiction on transnational Cybercrime, the researcher recommends the following measures to be taken.

- ✓ States should allow their Courts greater discretion when determining which Country should have Jurisdiction over Cybercrimes.
- ✓ States and international organizations should incorporate provisions that deal with resolving conflicts of Jurisdiction in international and regional agreements.

- ✓ International organizations and States should allow for the borderless application of international law, i.e., the territoriality principle of Jurisdiction, when prosecuting Cybercrimes and creating international tribunals or Courts specifically designed for prosecuting Cybercrimes.
- ✓ International organizations such as the United Nations should strengthen Cooperation between States in exercising the territoriality principle on transnational Cybercrime.
- ✓ States should work towards capacity building in the investigation and prosecution of transnational Cybercrimes, considering the unique nature of the technology. States should also enter into such agreements to avert the impunity of the perpetrator of the crime from justice.

Bibliography

Laws

- African Union Convention on Cyber Security and Personal Data Protection, Addis Ababa, Ethiopia, April 8-11, 2019.
- League of Arab States, Arab Convention on Combating Information Technology Offenses 5-9, Dec. 21, 2010 (entered into force Feb. 7, 2014**)**
- Computer crime proclamation no 958/2016, 22nd Year No. 83 Addis Ababa 7th July 2016.
- Computer Misuse Act 1990. The National Archives. 20 October 2010.
- Council of Europe. (2013), Convention on Cybercrime, ETS No. 185.
- Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse Lanzarote, 25.X.2007
- General Statutes of North Carolina, Section 14-453.
- German Information and Communications Services Act (IuKDG), 1997, Bundesgesetzblatt Teil I, Nr. 57/1997.
- Proclamation No. 414/2004, Federal Negarit Gazeta, Addis Ababa, 9th May 2005.

Books

- Calderoni, F.(2010).*The European legal framework on Cybercrime: striving for effective implementation*, Crime, Law and Social Change, 54(3).
- Cedric Ryngaert(2015), *Jurisdiction in International Law,* 2nd Edition, Oxford University Press, Pro Catherine Redgwell et al. eds.
- Cristos Velasco (2022), *Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments,* ERA Forum.
- Fotso, O., Yagan, S., Ryu, E., & Choo, K. R. (2016). Examining Cybercrime and cyber security trends in Africa. Journal of Cybersecurity, 2(1).
- Gideon Boas (2012), *Public International Law Contemporary Principles and Perspectives,* Edward Elgar Publishing Limited.

- Handelman, D. (2004). *The Sliding Scale of Test Transnational and Territoriality Principle*. In K. W. Weiler & J. Gilliom (Eds.), *International human rights law: Philosophical perspectives* Oxford: Oxford University Press.
- Jan Kleijssen and Pierluigi Perri(2017),*Cybercrime, Evidence and Territoriality: Issues and Options*. Kuijer and W. Werner (eds.), Netherlands Yearbook of International, T.M.C. Asser Press.
- Malcolm Shaw (2008), *International Law,* Cambridge university press, Sixth edition.
- McCusker, R. (2007). *Transnational organized Cybercrime: Distinguishing threat from reality*. Springer Science + Business Media B.V.
- Nicholas Tsagourias(2022), *The Legal Status of Cyberspace; sovereignty redux*, Research handbook on international law and Cyberspace, Nicholas Tsagourias and Russel Buchan(Ed), Edward Elgar Publishing Limited.
- United Nations Conference on Trade and Development (UNCTAD). (2012). Measuring the Impacts of Information and Communication Technology for Development. Geneva, Switzerland: United Nations.
- Wall, D (2001), Crime and the Internet Crime, cybercrime and cyber-fears, 1st edition, Routledge.
- Wall, D. (2007). Cybercrime: The transformation of crime in the information age. Polity: Cambridge University Press.
- Wilson, K. (2020). *Transnational Crime.* In Alexander Lautensach & Sabina Lautensach (Eds.), International Criminal Law: Cases and Materials 2nd Edition, Oxford University Press.

Journal Articles

- Armando A. *Cottim (2010), Cybercrime, Cyberterrorism, and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime*, European Journal of Legal Studies, 2010, vol 2, issue 3.
- Baglesman, Robert. (2014). *Hot Spots, Cool Responses: Transnational Cyber Crime and the Territoriality Principle.* Northwestern University Law Review, 108(3).
- Baker, A., & Chen, K.-H. (2013). *Transnational Cyber Crime and the Subjective Territoriality Principle*. International Criminal Justice Review, 23(1).
- Barker, J. (2018). *Modern Territorialism: Exploring the Role of Territoriality Principle in Transnational Cyber Crime Cases*. International Law Studies, 94(284).
- Brenner, Susan (2005), *Approaches to Cybercrime Jurisdiction,* Journal of High Technology Law. vol 6. Issue 1.

- Devlin Balko (2018), *State or Nation? Assessing Jurisdiction Over Transnational Cybercrime*, Brigham Young University Law Review.
- Elissa A. Okoniewski (2002), *Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet*, American University International Law Review Volume 18 | Issue 1 Article 6.
- Ella Shoshan (2014), *Applicability of International Law on Cyber Espionage Intrusions,* Faculty of Law Stockholm University,
- Griesser, D., Grünfeld, L., & Voigt, S. (2017). *The challenges of international cybercrime prosecution: Reflections on territoriality in a globalized world*. International Journal of Cyber Criminology, 11(2).
- Guske, I., Oh, N.-K., & Urban, L. (2008). *Applying 'Objective' Territoriality Principle: Analysis of Transnational Cybercrime Case in International Law*. Journal of Computer and Law, 21(4).
- Hoffman, P., Nuijten, M., & Ying, F. (2020). *Cybercrime: Cross-Border Cooperation and Extraterritorial Enforcement.* International Studies Quarterly, 64(3).
- Holt, T.J., Simons, W., Kalra, A., King, P. and Zhang, H. (2016). Effective Implementation of the Territoriality Principle: Responding to Transnational Cybercrime. Journal of International Criminal Justice, 14(3).
- Ikenga K. E. Oraegbunam (2016), *Towards containing the jurisdictional problems in Prosecuting cybercrimes: case reviews and responses*, NAUJILJ, volume 7.
- Jared A. Deifik & Bryan S. Turner (2015), *Applying Territoriality Principles to Transnational Cyber Crime: A Proposal for International Legal Harmonization*, 39 Vermont Law Review.
- Johnson, J.E., & Post, D.G. (2009). *Transnational Cybercrime: The Evolving Threat of the 21st Century*. The Howard Journal of Criminal Justice, 48(1).
- Jonathan Clough (2013) *A world of difference: the Budapest Convention on Cybercrime and the Challenges of harmonization,* Monash University Law Review (Vol 40, No 3).
- Jun Li and Jidong Jia(2018), *Confusion and Relief of Criminal Jurisdiction of Cybercrimes*, School of Law, Huazhong University of Science and Technology.
- Khalifa, Abdelmonem (2020). *Overcoming the Conflict of Jurisdiction in Cybercrime*. American University in Cairo, Master's thesis. AUC Knowledge Fountain.
- Kreiss, D. (2014). *A Vision of and for the Networked World: John Perry Barlow's Declaration of the Independence of Cyberspace at Twenty*. In J. Bennett, P. Kerr, and N. Strange (Eds.), Media Independence: Working with Freedom or Working for Free? New York, NY: Routledge

- Lan, Guobin & Ling, Polun. (2007). *Transnational Cybercrime and Territoriality Principle: An Analysis of Minimum Contacts Test Regarding Extraterritorial Heat in Cyberspace*. International Journal of Cyber Criminology, 1(1).
- Lei, Dong-hoon Thomas (2017), *Intergovernmental Cooperation in Transnational Cybercrime Investigations: Exploring Challenge*s., Third World Quarterly, Vol. 38 Issue 9.
- M N. Schmitt (2014), *The Law of Cyber Warfare: Quo Vadis?* Stanford Law & Policy Review. Volume 25, issue 269.
- Macfarlane, E. (2020). *The Transnational Cybercrime and Territoriality Principle: A Minimum Contacts Test.* available on https://cyberlawclinic.blog/2020/08/11/the-transnational-cybercrime-and-territoriality-principle-a-minimum-contacts-test/ accessed on 01 January 2022.
- McCarthy, B. (2019). *Transnational Cybercrime: Challenges in Establishing Territoriality in Criminal Jurisdiction*. International Criminal Law Review, 19(4).
- McDowell D, (2015). *Defying Territory: Transnational Cybercrime and Transnational Governance*. University of New South Wales Law Journal 156.
- Meetali Rawat(2021), *Transnational Cybercrime: Issue of Jurisdiction*, International Journal of Law Management & Humanities, Vol. 4 Issue 2.
- Mohamed Chawki. "A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy." METU Faculty of Law, Mersin University, 2013,
- Moore, T.J., Anderson, R.B. & Parsons, C. (2011). *Cyber calcification: locating Cybercrime in a transnational law enforcement context*. International Journal of Law, crime, and Justice, 39(3), 183-198.
- Morson, C., & Allen, E. A. (2009). *United States v. Almblad: Sentencing a Terrorist as an Ordinary Criminal--An Unconventional Outcome in an Unorthodox Case*. University of Michigan Journal of Law Reform, 42(3).
- Nadina Foggetti(2008), *Transnational Cybercrime, differences between national laws and development of European legislation: by repression?*, in Masaryk University Journal of Law and Technology, Fall.
- Osman Goni(2022*), Cyber Crime And Its Classification*, International of Electronics Engineering and Applications, Vol. 10, No.1
- Peerenboom, R.P(2014), *Business and human rights: implications of jurisdictional regimes for economic activities with a transnational dimension*. Comp. J Int'l & Com L. 28.

- Plattner, M., Bürger, D., Reichel, P., & Schwald, S. (2013). *Transnational crimes in Cyberspace and the principle of territoriality*. Computer Law & Security Review, 29(3).
- Rollin Perkins (1971), *The Territorial Principle in Criminal Law*, Hastings L.J.
- Rozeman, C. (2015). *Application of the Principle of Subjective Territoriality in the Fight against Transnational Cybercrime*. Journal of International Criminal Justice, 13(3).
- Satwinder Kaur(2013), *Determining Jurisdiction of Cyber Crimes: Challenges and Issues*, International Journal of Research in Engineering and Technology, vol 2.
- Serhii S. Cherniavskyi et al, (2019) *International Cooperation in the Field of Fighting Crime: Directions, Levels, and Forms of Realization*, Journal of Legal, Ethical and Regulatory Issues, Vol: 22 Issue: 3.
- Shqair, Y. (2020). *Cybercrime Laws in Arab Countries Focus on Jordan, Egypt, and the UAE.* Fredrich Naumann Stiftung.
- Sigler, Anja E. (2018), *Implementing Intergovernmental Cooperation for Cyber Crime Investigations: The Significance of Territoriality*, European Journal of Enforcement, vol. 6, no. 2.
- Singh, P. (2019). *Subjective Territoriality: Negotiating Meaning, Rules, and Order in the Low-Income City*. Singapore Journal of Tropical Geography.
- Smith, L.P. (2018). *The Fight Against Transnational Cybercrime: International and National Efforts*. Santa Clara Computer & High Technology Law Journal, 34(2),
- Sunil. C. Pawar et al (2021), *Cyber Crime, Cyber Space and Effects of Cyber Crime*, International Journal of Scientific Research in Computer Science Engineering and Information Technology, Volume 7, Issue1.
- Teske, D., Lindblom, J., & Harrington, C. (2018). *Objective territoriality in transnational Cybercrime: Practical cases from the United States*. International Journal of Cyber Criminology, 12(2).
- Thomson, D. (2006). *Global Constitutionalism: Cyber Crimes, Territorial Sovereignty, and International Conflict?* University Of Toronto Law Journal, 56(1), 75-119.
- Toni M. Mastrobueni, Sally MacIntyre(2016), *Cybercrime Law and the International Framework: A Transnational Analysis,* ICMCP Journal of Cybersecurity & Privacy.
- Uchenna Jerome(2019) *The African Union Convention on Cyber Security: A Regional Response towards Cyber Stability,* Masaryk University Journal of Law and Technology, vol. 5, no. 1.
- Verdi, E., & de Hert, P. (2018). *The effects test Applying the territoriality principle of international law to transnational Cybercrime.* International Review of Law, Computers & Technology, 32(3).

- Veridiana Alimonti(2022) Assessing *New Protocol to the Cybercrime Convention in Latin America: Concerns, Human Rights Considerations, and Mitigation Strategies*, Electronic Frontier Foundation.
- Wang, Kang-Kwong(2008). *Transnational Cybercrime and the Territoriality Principle*. Journal of International Banking Law and Regulation, vol. 23, 2008,
- Wendell Berge(1931), *Criminal Jurisdiction and the Territorial Principle*, Michigan Law Review, The Michigan Law Review Association Vol. 30, No. 2.
- Yen, C. (2014). *How the Syrian Electronic Army is shaping international politics*. Journal of Contemporary Studies, 3(2), 37-45.)

Thesis

- Afnan Alabdulatif (2018), *Cybercrime and analysis of Laws in Kingdom of Saudi Arabia*. Master of Science in Information System Security Faculty of the Department of Information and Logistics Technology the University of Houston.
- Neethu N(2020), *Role of International Organizations in Prevention of Cyber-Crimin*als, University of Law Hyderabad.
- Qianyun WangA (2016), *Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*, Erasmus University Rotterdam.
- Iyasu Teketel(2018), *Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences*, A Thesis Submitted to the School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Masters of Law (LL.M) in Public International Law.

Reports and others

- Ana Cerezoa, Javier Lopez and Ahmed Patel (2007), *International Cooperation to Fight Transnational Cybercrime*, Conference Paper.
- Ashabari Basu Thakur, Determination of Jurisdiction in Cyber - Crimes: Issues and Challenges available on https://www.legalpedia.co.in/articlecontent/determination-of-jurisdiction-in-cyber-crimes-issues-and-challenges.html accessible on 23 march 2023.
- Cybercrime Magazine (2020), Special Report: Cyberwarfare in the C-Suite. Steve Morgan (Eds),https://cybersecurityventures.com/hackerpocalypse-cybercrime-report- accessed 25 September 2022.

- European treaty series no 185, Explanatory Report to the Convention on Cybercrime Budapest, 23. XI.2001.
- General assembly resolution 55/63. Combating the criminal misuse of information technologies.
- General Assembly resolution 65/230 Twelfth United Nations Congress on Crime Prevention and Criminal Justice.
- H.E. Ms. Faouzia Boumaiza Mebarki, *Letter to the UN Ad Hoc Committee on Cybercrime, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose*, available on https://www.hrw.org/news/2022/01/13/letter-un-ad-hoc-committee-cybercrime.
- Prof. Dr. Kennedy Gastorn(2017*), Relevance of international law in combating cybercrimes: current issues and AALCO'S approach*, Presentation at the 4th World Internet Conference.
- Saloni Khanderia(2020), *The curious case of personal Jurisdiction for cyber-based transnational transactions in India: Does one size fit all?* Available at https://conflictoflaws.net/2020/the-curious-case-of-personal-jurisdiction-for-cyber-based-transnational-transactions-in-india-does-one-size-fit-all/ accessed on 02 May 2023.
- Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World states Brazil, from 12 to 19 April 2010.
- U.S. Department of Justice "*Czech National Pleads Guilty to Attempting to Hack into US Government Computers*" US Department of Justice, August 2nd, 2018 available at https://www.justice.gov/usao-ut/pr/czech-national-pleads-guilty-attempting-hack-us-government-computers accessed n 02 January 2022.
- UNGA *'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (24 June 2013) UN Doc A/68/98 paras 19–20.
- United Nations Office on Drugs and Crime. (2013, February*). Comprehensive Study on Cybercrime.* Draft. Ilias Bantekas & Susan Nash (2003), International Criminal Law, 2nd Edition, Cavendish Publishing Limited.

Cases

- American Banana Co v. United Fruit Co., 213 US 347 (1909).
- Blakey v. Continental Airlines, Inc., 992 F. Supp. 731 (D.N.J. 1998).
- Calder v. Jones, 465 U.S. 783 (1984)
- Lotus (France v. Turkey), PCIJ series A, no. 10, p. 4 (1927).
- United States v. Aleksei Burkov, 1:15-cr-00245-TSE,2020
- Moriarity v. Wilson,72 F. Supp. 3d 1245 (D. Colo. 2012)
- Nikulin, 2018 USDC NDCA 15-00249, United States District Court for the Northern District of California.
- United States Attorney's Office, Southern District of New York, U.S. v. Lauri Love, S2 13 Cr. 367 (LAK) (Indictment), 15 July 2013.
- United States v. Aleynikov, No. 11-1126 (2d Cir. 2012)
- United States v. Almblad (546 F.3d 940 (2008)
- United States v. Seleznev, 820 F.3d 1094 (9th Cir. 2016I)
- Yahoo! France and Yahoo! Inc. v. License (Tribunal de Grande Instance, 24th Ch., Judges Mareille Déchamps, Christine Bitquenne-Leroy, André Delattre, Jean-Noël Gombaud, Arnaud Gilluin, Françoise Bairin Courbet & Jean-Daniel Politi), No. 2001/10455 (February 20, 2002).
- Zippo Mfg. Co. v. Zippo Dot Coin, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

Magazine

- Alan Elsner (2000), *Virus Attack Causes Billions in Damage,"* Reuters, May 15, 2000. Available on https://www.reuters.com/article/us-virus-attack-costs/virus-attack-causes-billions-in-damage-idUSL15116450 accessed on 16 January 2023
- Asphyxia Webb(2014), *International Efforts to Combat Transnational Cybercrime*, Available at: http://lawthinktank.weebly.com/international-efforts-to-combat-transnational-cybercrime--an-overview.html accessed on 13 January 2023.
- Cyber-attack: US and UK blame North Korea for WannaCry, available on https://www.bbc.com/news/world-us-canada-42407488 accessed on 23 April 2023.
- Gahutan, M. (2009). *The Anti-Virus Law of the Philippines. Malaya Business Insight*, retrieved on 11 February 2010 from www.malaya.com.ph/apr14/tech1.html accessed on 18 January 2023.

- Nakashima, Ellen (2016). "Syrian hacker extradited to the United States from Germany". Washington Post Available on https://www.washingtonpost.com/world/national-security/syrian-hacker-extradited-to-the-united-statesfromgermany/2016/05/09/eb855654-15fa-11e6-aa55-670cabef46e0_story.html accessed on 01 January 2023.
- Paris prosecutor's office charges Facebook for 'failing to remove criminal hate speech content' from its platform." The Guardian. Guardian News and Media, 24 Jan. 2021, available on www.theguardian.com/technology/2021/jan/24/paris-prosecutors-office-charges-facebook-for-failing-to-remove-criminal-hate-speech-content/. Accessed on 01 January 2022.
- Sill, S. (2016, December 7). *Ideas for International Cooperation and Collaboration Before Dealing with Transnational Cybercrime.* The Good Men Project. Retrieved from https://goodmenproject.com/featured-content/ideas-for-international-cooperation-and-collaboration-before-dealing-with-transnational cybercrime/
- *Stanislav Lisov Guilty of Cybercrime in Europe,* Cyber Defense Magazine, May 17, 2019, available at https://www.cyberdefensemagazine.com/stanislav-lisov-guilty-of-cybercrime-in-europe/. Accessed on 20 December 2022.
- Tonya Riley, *The Cybersecurity*, Washington post-2020 Dec.7, 2020, available on https://www.washingtonpost.com accessed on 08 February 2021.

Website

- https://www.washingtonpost.com
- https://www.itpro.co.uk/it-legislation
- http://www.lasportal.org/ar
- www.unodc.org/documents/commissions