UCC Law Journal. Volume 3 Issue 1 Jul. 2023, pp. 119-151
DOI: 10.47963/ucclj.v3i1.1253

UNIVERSAL JURISDICTION FOR TRANSNATIONAL CYBERCRIMES?

Flora Alohan Onomrerhinor[1]

ABSTRACT

Transnational cybercrimes (TNCCs) are cybercrimes occurring across several jurisdictions. The advancement of technology has brought about an increase in the sophistication, severity and comprehensiveness of incidents of cybercrimes such that cybercrimes can now be effortlessly transnational. In the main, however, the various legal responses to TNCCs have shown States consistently applying traditional territorially based rules to online activities by enacting laws that do not adequately address the borderless nature of the Internet. This paper examines the jurisdictional challenges of transnational cybercrimes as well as the inadequacies of present legal responses to transnational cybercrime. With the aid of the doctrinal research methodology (legal analysis), it finds that purely domestic legal responses to cybercrimes, no matter how advanced, are inadequate as a fragmented approach cannot effectively eradicate the problem created by the presence of safe havens. It concludes that a holistic approach is needed and recommends the adoption of a global instrument with international recognition of universal jurisdiction for serious categories of TNCCs capable of compromising international Peace and security, such as cyber terrorism, hacking and the creation and dissemination of malicious codes targeting critical infrastructures or leading to the denial of essential services.

Keywords: Jurisdiction, Cybercrime, Transnational, Challenges, Domestic, States

INTRODUCTION

The term transnational when used to describe an activity means any activity that originates from within a given society, is commissioned and undertaken by agents operating in several national jurisdictions and transmitted or replicated across national borders. Crime according to the United Nations Convention on Transnational Organized Crime refers to

[1] PhD, LLM, LLB, BL, Senior Lecturer, Department of Jurisprudence and International Law, Faculty of Law, University of Benin, Benin City, Nigeria, E- mail: flora.alohan@uniben.edu, +234 703 442 8226.

any conduct (an act or omission) constituting an offence according to the laws adopted by states and international organizations. Article 2 of the Convention broadly defined transnational crimes to cover not only offences committed in more than one state but also those that take place in one state but are planned or controlled in another. It also includes crimes that are committed in one state by groups that operate in more than one state as well as crimes that are committed in one state but have an impact on other states. Cybercrimes are crimes committed by means of the Internet and TNCCs are cybercrimes that occur across several jurisdictions.

The advancement of technology has brought about an increase in the severity, comprehensiveness and sophistication of incidents of cybercrimes such that cybercrimes are now effortlessly transnational. At present and with the right technology and technical know-how, cybercrime has the potential to be so devastating as to literarily cripple countries' defence systems or compromise international peace and security. Singapore's Ministry of Defence breach,[2] along with the growing incidence of cyber-attacks around the world from those of Ukraine's power grid[3] all the way to the electoral process of the United States,[4] has made it clear that the challenge is likely to rise even further in the coming years.[5]

Most countries have responded to this challenge by enacting legislation to address cybercriminal conduct. In the main, however, these legislations have shown States

[2]On the 28th of February 2017, the Singapore's Ministry of Defence reported that its systems had been compromised resulting in the loss of personal data of 850 national service and employees. Although no classified military data was stolen, it was reported that the purpose of the attack was to steal military secrets. See Niranjan Arasaratnam, Adrian Fisher and Chung Yee Gui, "Singapore: Cybercrime Law Strengthened" Linklters, June 14, 2018, www.linklaters.com/en/insights/publications/tmt-news-june2017/singapore-cybercrime-law-strenghtened/.

[3] In December 2016, hackers took down a part of Ukraine's power grid, living over 230,000 residents of Ivano-Frankivsk region of the Western Ukraine without power for over an hour. See Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" Security, accessed September 18, 2018, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-unkraine-power-grid/.

[4] It was alleged that the Russian cyber-attack on the Democratic National Committee, a cyber-espionage and information-warfare devised to disrupt the 2016 presidential election, harmed one candidate, Hilary Clinton and tip the election in favour of her opponent, Donald Trump. See Eric Lipton, David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times, December 13, 2016, accessed September 18, 2018, http://www.nytimes.com/2016/12/13/us/politics/russians-hack-election-dnc.html.

[5]Prashanth Parameswaran, "Singapore Ramps Up its Cyber War" The Diplomat, accessed June 14, 2018 http://thediplomat.com/2017/03/Singapore-ramps-up-its-cyber-war.

consistently applying traditional territorially based rules to cybercrimes and refusing to treat the Internet as borderless. This paper employs a doctrinal methodology in its analysis of a paradigm shift. It examines the jurisdictional challenges of transnational cybercrimes, the inadequacies of present legal responses to transnational cybercrime and the possibility of international recognition of universal jurisdiction for serious categories of TNCCs.

It is divided into six parts. The first part is the introduction. The second discusses the concept of jurisdiction in international law. The third identifies the jurisdictional challenges of TNCCs. The fourth discusses the inadequacies of most legal responses to TNCCs. The fifth part justifies the recognition of universal jurisdiction for some categories of TNCCs and the last part contains the recommendation and conclusion.

MEANING OF JURISDICTION

Jurisdiction is a state's legitimate assertion of authority to affect legal interests.[6] It refers to a state's authority under international law to regulate the conduct of persons, natural and legal, and to regulate property in accordance with its municipal law.[7] The five bases ordinarily relied on by States to assert jurisdictions over crimes are territorial principle, nationality principle, protective principle, passive personality principle and the universality principle.

Territorial Principle

Territorial jurisdiction also called territorial principle expresses the overall control a State has over its territory.[8] It allows a State to prosecute crimes that have occurred wholly or partially within its territory. It expresses the exclusivity or absoluteness of the power of state over its territory and this was captured in the case of *Schooner Exchange v McFaddon*.[9] Crimes alleged to have been committed within the territory of a state may come before its

[6] Mehmet Zülfü Öner, 'The Principle of 'Universal Jurisdiction' in International Criminal Law' (2016) 7 Law & Justice Rev 177
[7] Malcolm N. Shaw, *International Law* (7th edn Cambridge, 2016) 469.
[8] Amos Enabulele and Bright Bazuaye, *Topics in Public International law* (Malthouse, 2019) 237.
[9] (1812)7 Cranch 116

domestic or municipal courts and the accused if convicted may be sentenced and punished. This is the case even where the offender is a foreign national.[10]

The inviolability of the territorial integrity or sovereignty of a state is one of the foremost principles of international law and the territorial jurisdiction of a state is thus protected from incursion at international law. A state may only within permissible limit, extend its jurisdiction beyond its territory by virtue of the exceptions under customary international law or existing treaty. [11]

The first basis for the exercise of jurisdiction under the Cybercrime Convention is the principle of territorial jurisdiction, where the offence is committed within the states territory. Thus, while a state may opt out of asserting jurisdiction on the basis of nationality or in respect of their ship or aircraft, it must exercise territorial jurisdiction.[12]

The exercise of territorial jurisdiction can be categorized into subjective and objective territorial principle.[13] Subjective jurisdiction is exercised by the state in which a crime was committed while objective territorial jurisdiction also known as objective territoriality is exercised by the state in which the crime had effect.[14] The latter allows a claim of jurisdiction for criminal conduct occurring outside the jurisdiction of a state but having substantial effect on that state.[15]

Nationality Principle

Nationality provides an essential link between the individual and the state that enables the state to legally perform actions that have significant impact on them.[16] The nationality principle allows a State to prosecute crimes committed by its own nationals outside of its

[10] See *Holmes v Bangladesh Binani Corporation*[1989] 1 AC 1112, 1137; 87 ILR 365, 380-381 per Lord Griffiths and Lord Browne- Wilkinson Ex parte Pinochet (No. 3) [2000]1 AC 147, 188; 119 ILR 60
[11] Enabulele and Bazuaye (n 7) 237.
[12] Article 22(2) of the Cybercrime Convention. See Jonathan Clough, *Principle of Cybercrime*, (Cambridge, 2015) 477.
[13] Enabulele and Bazuaye, *Topics in Public International law* (n 7) 239.
[14] ibid
[15]Clough, *Principles of Cybercrime* (n 11) 476.
[16] Shaw, *International Law* (n 6) 479.

territory. This is sometimes known as the "active personality principle".[17] This principle of jurisdiction is predicated on the fact that a bond exist between a state and its nationals which bond or link remains unbroken even when the said nationals are outside the state of their nationality.[18]

This link enables the state to extend its jurisdiction to its nationals beyond its boundaries and to invoke its jurisdiction over them for the violation of its laws notwithstanding the fact that they are outside its territory.[19] This makes it possible for a state to supervise and regulate the acts of its citizens both within and within permissible limits, without its territory so long as the national remains a citizen of the state exercising jurisdiction.[20]

The nationality principle is a basis for the exercise of jurisdiction under the Cybercrime Convention. Under Article 22(1)(d) of the Convention, a party can establish jurisdiction where the offence is committed by one of its nationals irrespective of where it occurs in the world.[21] In the same vein, section 1, 2, 3,3A and 3ZA of the UK Computer Misuse Act of 1990 and sections 41 – 44 of the UK Serious Crime Act 2015 contains provisions for extraterritorial jurisdiction on the basis of nationality.

Protective Principle

Under this principle of jurisdiction, States may assert jurisdiction over crimes committed abroad by foreign nationals which constitute a threat to some fundamental national interest or security of the State seeking jurisdiction. The extent to which this principle is accepted as justifying the assertion of jurisdiction depends on the crimes in question.[22]
This principle is often justified on the ground that acts committed by non-national of a state outside the said state could have prejudicial effects on the state's security or affect vital

[17] Quang Trinh, Hugh Bannister and Meg O'Brien, *The Principle of Universal Jurisdiction* (Mallesons Stephens Jaques ed Australian Red Cross, 2010) 5.
[18] Enabulele and Bazuaye, *Topics in Public International law,* 241.
[19] ibid see *Blackmer v United States* (1932) 284 U. S. 421, 438 where the United States' Supreme Court held that the United States have jurisdiction over its absent citizens and they are bound to take notice the laws that are applicable to them and obey them.
[20] ibid
[21] Clough, *Principles of Cybercrime* (n 11) 477.
[22] Enabulele and Bazuaye, *Topics in Public International law* (n 7) 41.

interest of that state. In *United States v. Pizzarusso*[23] the United States Court of Appeal second Circuit held that false statements on an immigration visa before a U.S. Consul in Canada had a sufficiently adverse impact on the United States' interest to warrant exercising jurisdiction over the defendant.[24]

Passive Personality Principle

The exercise of jurisdiction under this principle of jurisdiction is based on the nationality of the victim. It allows a State to punish foreign nationals for acts committed abroad which are harmful to the State's nationals. This principle of jurisdiction may be invoked by a state to try offenders for offences committed against its nationals abroad.[25]

The assertion of jurisdiction on this basis is said to arise out of the duty of a state to protect its nationals abroad and the need to address the crime's effect irrespective of where it took place.[26] States can exercise extraterritorial jurisdiction under this principle for crimes committed outside their territory if they can establish a connection with the act in question. In this case the state seeking to exercise jurisdiction must be able to show that it suffered significant harm from the criminal act in question.

Universality Principle

The universality principle also referred to as universal jurisdiction has been described as the legal principle allowing or requiring a state to bring criminal proceedings in respect of certain crimes irrespective of the location of the crime and the nationality of the perpetrator or the victim.[27] Universal jurisdiction is the right of a state to 'define and prescribe punishment for certain offenses recognized by the community of nations as of universal

[23] 388 F.2d 8(2d Cur.1968

[24] See also *United States v Fernandez* [1974], 496 Cir. F.2d 1294. Here, the defendant was charged with possessing, forging and altering stolen United States Treasury checks. The defendant argued that the United States courts lacked jurisdiction because all the criminal acts involved were alleged to have taken place in Mexico. The court noted that the defendant's acts could prevent the normal disbursement of funds to those lawfully entitled to receive such funds and in recognition of this fact the court held that the United States had jurisdiction over the defendant

[25] ibid, 243

[26] See Enabulele and Bazuaye, *Topics in Public International law* (n 7) 243, John G. McCarthy, 'The Passive Personality Principle and Its Use in Combating International Terrorism' (1981) 13 Fordham Int. Law J 298, 301.

[27]Öner, 'The Principle of 'Universal Jurisdiction' in International Criminal Law' (n 5) 174.

concern' regardless of whether the prosecuting state can establish a connection with the perpetrator, victim, or location of the offense.[28]

Here, there may be no connection whatsoever between the crime and the state wishing to prosecute, other than the fact that the prosecuting state believes that the crime is such that it should not go unpunished and the states with the necessary connections may have no facility to prosecute or are not interested in prosecuting. This is unlike the four other principles of jurisdiction which attaches to the extraterritorial conduct of some form of connection on the basis of either territory or nationality.[29]

Universal jurisdiction is conferred by international law and usually contained in treaties of criminal nature empowering state parties to such treaties to exercise jurisdiction over certain crimes whenever the perpetrator comes in contact with the jurisdiction of the states.[30]

International treaties, agreements and conventions have provided universal jurisdiction over a number of offences, such as hijacking and torture. It can also be a matter of customary international law. Treaties, agreements and conventions with provisions for universal jurisdiction often contain an obligation to prosecute or extradite the offender. This obligation is referred to as the principle of *aut dedere aut judicare*. The principle *aut dedere aut judicare* by definition entails the duty of the state concerned to extradite or to prosecute the accused.[31]

The exercise of universal jurisdiction has not been without some difficulties. The primary concern is that the prosecuting State will be infringing upon the jurisdiction, and sovereignty of States with more direct connections with the crime.[32] Other concerns associated with the use of this principle of jurisdiction include; legitimacy, practicality and political ramifications of a prosecuting State exercising universal jurisdiction when it has no direct interest in the crime.[33]

---

[28] Ibid 178.
[29] Enabulele and Bazuaye, *Public International Law* (n 7) 244. Also see Kenneth C. Randall, 'Universal Jurisdiction under International law' (1988) 66 Tex Law Rev 785-788.
[30] ibid
[31] Öner, 'The Principle of 'Universal Jurisdiction' in International Criminal Law' (n 5) 179.
[32] ibid
[33]ibid

There are a handful of international crimes for which universal jurisdiction is widely accepted as a matter of customary international law. They include piracy (the first crime to be subject to universal jurisdiction), genocide, torture, war crimes and crimes against humanity.[34]

One rationale for the existence of universal jurisdiction is that certain crimes are so heinous that they have been universally condemned by states, or offend the international community as a whole by infringing universal values, and so all States have an interest in punishing those crimes wherever they occur regardless of the nationality of the suspect or victims.[35] Thus, we find its use in relation to such crimes as piracy and terrorism. More often than not, the justification for the exercise of this principle of jurisdiction correlates with the idea that the violation of such fundamental obligations offends all states.[36]

In a study carried out by Amnesty International in 2011, a preliminary survey of the 193 states of the United Nations Organization revealed that approximately three-quarters (about 145 states) of the United Nations member states have authorized their courts to exercise universal jurisdiction over one or more crimes under international law and that almost half have authorized their courts to exercise universal jurisdiction over ordinary crimes. None of the states made formal objections to the enactment of such criminal legislation recognizing the use of a universal jurisdiction.[37] This survey is an indicator of states' capacity to use the principle of universal jurisdiction in fighting impunity and ensuring justice.

[34]Universal jurisdiction for genocide, torture, war crimes and crimes against humanity have been recognized in some treaties such as Convention on the Prevention and Punishment of the Crime of Genocide, for genocide and Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, for torture. See also *Question Relating to the Obligation to Extradite or Prosecute (Belgium v. Senegal),* judgment of the ICJ, July 12, 2012, where Belgium's claim that Senegal breached its obligation to exercise universal jurisdiction provided for in Article 5(2) of the Torture Convention was upheld.

[35] ibid.

[36] See Christopher C. Joyner, 'Arresting Impunity: The case for Universal Jurisdiction in Bringing War Criminals to Accountability' (2007) 59 Law and Contemporary Problems 153, 169. Also see Michael P. Scharf, 'Universal Jurisdiction and the Crime of Aggression' (2012) 53 Har. Int'l L. J.367 here, Scharf stated the two premises underlying universal jurisdiction as being the gravity of the crime and place of the act.

[37]Amnesty International, *Universal Jurisdiction: The duty of States to Enact and Enforce Legislation* (AI Index, 2001)1.

UCC Law Journal. Volume 3 Issue 1 Jul. 2023, pp. 119-151
DOI: 10.47963/ucclj.v3i1.1253

JURISDICTIONAL CHALLENGES OF TRANSNATIONAL CYBERCRIMES

According to Weber, the jurisdictional problems in the prosecution of cybercrime manifest itself in three ways: lack of criminal statutes, lack of procedural powers and lack of enforceable mutual assistance provisions with foreign states.[38] While it may no longer be accurate to say that there is a complete absence of legal and technical facilities for the prosecution of cybercrimes, it is true that the inadequacy of existing facilities for the investigation and prosecution of cybercrime, especially transnational cybercrimes, constitutes a challenge.

Absence of, or Inadequacy of Cybercrime Specific Legislation in Some States

Recently at the 2nd African Forum on Cybercrime held in June 2021, it was stated that the major challenges to the effective prosecution of cybercrime can be found in policy and legislation; the majority of which stem from the absence of common understanding on cybercrime among criminal justice authorities, coherent cybercrime legislation harmonization, shared definition on cybercrime, sufficient standardization which results in identification, collection and use of e-evidence and admissibility issues.[39]

No other type of crime can become transnational so effortlessly like cybercrime.[40] Even where the offender and the victim are in the same jurisdiction, evidence of the offence may pass through or be stored in other jurisdictions. As a result of this, it is important that there be some degree of harmonization between countries in order to effectively regulate cybercrimes. This is because harmonization will help to eliminate safe havens and increase cooperation among states.

Significantly, a lot has been done in the African region since the United Nations' General Assembly's Resolution 55/63 of 4th December 2000 which called on states to ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies. As at 2016, 22 countries have enacted cybercrime legislation and the number is increasing by the day. Although a good number of states in the African region and beyond, have enacted cybercrime specific legislation in the last decade and others are updating

[38] Amelia M. Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 Berkeley Technol. Law J. 425.
[39] Clough, Principles of Cybercrime (n 11) 478.
[40] ibid

existing ones,[41] there are still some that are yet to do so.[42] States that are without adequate cybercrime laws constitute safe havens for cybercriminal.[43]

The presence of safe havens presents a major challenge in the fight against cybercrime. It remains one of the foremost jurisdictional issues constituting a challenge to the effective prosecution of transnational cybercrime. In a survey carried out by the Council of Europe on the current state of cybercrime legislation in the African region, in 2016 for instance, a cursory overview of 54 countries of the region in terms of specific criminal law provisions on cybercrime and electronic evidence revealed that only 11 States[44] had basic substantive and procedural law provisions in place, a further 12 States[45] had substantive and procedural law provisions partially in place while the majority of the states of the region did not have specific legal provisions on cybercrime and electronic evidence in force. Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States[46] and in some instances, bills had been presented to national parliaments, in others the fate of draft laws were uncertain.[47] States without cybercrime specific legislations act as safe havens for cybercriminals and reduces the effectiveness of cybercrime legislations in countries with advanced cybercrime legislations. At the time of the report, 17 states[48] in the

[41] Mauritius is currently updating it laws on the subject
[42] N. Kshetri, 'Cybercrime and Cyber security in Africa' (2019) 22 Journal of Global Information Technology Management 77.
[43] According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and deal with electronic evidence. Law enforcement officials in some countries do not take major actions against hackers attacking international websites. Zimbabwe introduced its Cyber Security and Data Protection Bill in May 2020.
[44] Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia.
[45]Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe.
[46] Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe.
[47]Council of Europe, 'Second African Forum on Cybercrime 2021' <www.https://coe.int/en/web/cybercrime> accessed October 15, 2021.
[48] Algeria, Equatorial Guinea, Gabon, Guinea, Guinea Bissau, Angola, Burundi, Cape Verde, Central Africa Republic (CAR), Comoros, Democratic Republic of Congo, Dibouti, Eygpt, Eritea.

African region alone, constituted safe haven for cybercrime as they had no statute prohibiting cybercriminal conducts.[49]

Significantly, some states have enacted cybercrime legislation in the last five years since the report was given. At the 2nd African Forum on cybercrime held recently in June 2021, it was reported that 41 countries in the African region now have substantive criminal law provisions partly or largely in place to deal with cybercrime and 16 countries have procedural legislation in place to secure evidence necessary for effective prosecution of cybercrime.[50] However, while it is true that some countries that once constituted safe havens have now enacted cybercrime specific legislation, the problem of safe haven is far from over.[51] It is still true that in spite of the increased awareness of the threat presented by cybercrime, states that are yet to enact statutes that specifically criminalize cybercrime constitute safe havens and present jurisdictional challenges to the prosecution of transnational cybercrimes.[52] At the same time, the speed of development coupled with its sophistication along with the increasing advance in technology continues to challenge the adequacy of present legal responses to cybercrime in States where such legislations exist. This shows that purely domestic response to TNCCs cannot effectively eliminate the problem of safe havens. In a study conducted by the United Nations Office on Crime and Drugs in 2013, over half of the responding countries stated that between 50 and 100 per cent of cybercrime acts that are encountered by their police involved a transnational element.[53]

Inadequate procedural powers

Procedural powers refer to specific procedural rules on investigation and preservation of evidence applicable in cyberspace such as expedited preservation of stored data, expedited

[49] E. F. G. Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (2016) 6 Journal of Internet and Information System 1.
[50] Mauritius is currently updating its laws on the subject.
[51] As of March 2018, countries such as Libya, Mali, Guinea Bissau, Sierre Leone, Togo, Eritrea, Gabon, Demoncratic Republic of Congo, Angola, Namibia, Swaziland, Lesotho, Central Africa Republic, Somalia and Comoros still constituted safe havens.
[52]M. Lucchetti, M. 'Cybercrime Legislation in Africa: Regional and International Standard' (GLACY+ - Global Action on Cybercrime Extended, April 12, 2018) <https://au.1nt>newsevents> 'accessed October 17, 2021.
[53]United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime: Draft February2013' <unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed May 18, 2019.

preservation and partial disclosure of traffic data, and interception of content data.[54] They include procedural mechanisms meant to enhance the legal capabilities of law enforcement authorities to investigate and prosecute cybercrime offences such as measures to facilitate the search, seizure, or preservation of digital evidence, or the interception of electronic communications.[55]

Real time evidence in the cyberspace is volatile and preservation has to be done in a short time. Unless there are evidentiary rules and provision for international cooperation on how such data is to be located and obtained (search and seizure), they can be lost very quickly. Evidence gathering in TNCC is a dynamic, broad and increasingly significant phenomenon that differs remarkably from evidence gathering in the traditional sense. Adequate procedural powers in the context of TNCCs require novel coercive measures, investigatory powers and tactics and technical methods that can only be achieved by adjusting traditional principles of procedural justice.[56]

For example obtaining real time evidence requires: the power of sudden search i.e, conducting digital forensic investigations against computers suspected to be sources or targets of cyber-attacks without judicial warrant where there are reasonable grounds to believe that computer crimes are likely to be committed; allowing courts to rule ex parte upon request by investigators for a production order against a person thought to be in possession of computer data needed for investigation, granting a production order even without the presence of the person concerned that could have legitimate reasons to protest an otherwise unreasonable request, disclosure of personal computer data in the course of enforcing such order which could violate data privacy rights; a mandatory duty to report that would prompt service providers to employ algorithmic bots to automatically detect illegality.[57]

Adequate procedural powers or facilities thus require a balance between the efficient criminal investigations and the rights of the individual which is almost impossible to find and

[54] D. Cangemi, 'Procedural law Provisions of the Council of Europe Convention on Cybercrime' (2004) 18 Int'l Rev Law Comput. Technol. 165.
[55] U. J. Orji, 'The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability,'(2018) 12 Masaryk Univ. J. Law Technol. 91.
[56] J. Riekkinen, 'Evidence of Cybercrime and Coercive Measures in Finland.' (2016) 13 Digital Evidence and Electronic Signature Law Review 49.
[57] ibid

uphold. This has led to criticism of the Budapest Convention and the Ethiopian Cybercrime Proclamation of 2016, the latter made provision for procedural and evidentiary matters like the preservation and production of computer data by service providers, rules by which computer data or systems could be searched, accessed and seized by investigators, rules on the admissibility of electronic evidence and related authentication procedures and cooperation with law enforcement bodies of other countries and organizations.[58] As a result of the above, most states are either unwilling or unable to make adequate procedural provisions for the investigation of TNCCs because they require constant adjustments as criminality, technology, and societies continue to evolve.

In addition, some states lack the resource and procedural tools necessary to conduct computer crime investigations (digital forensic and technical surveillance). In a November 2016 report of the African Union Commission and the Cyber security firm Symantec, about 30 countries in the African region for example lack procedural provisions to deal with electronic evidence in the fight against cybercrime.[59]

The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications. The complexities of these technologies and their constant and rapid change mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions. Recently, Mauritius reported a steep increase in the number of cybercrime offences as a result of the technical challenges that its prosecution presented law enforcement agencies and prosecutors. This challenge was only surmounted by the training initiative of the Council of Europe GLACY + project.[60]

Given the quickly evolving nature of computer technology, countries must continue to increase their computer forensic capabilities which are essential in computer crime investigations. With the speed at which communication technologies and computers evolve, prompting rapid evolution in criminal tradecraft, experts must receive regular and frequent

[58] K. Yilma, 'Some Remarks on Ethiopia's New Cybercrime Legislation' (2016) 10 Mizan Law Rev 448.
[59]Kshetri, 'Cybercrime and Cyber security in Africa' (n 41) 77.
[60] Council of Europe, 'Second African Forum on Cybercrime 2021' (n 46)

training in the investigation and prosecution of high-tech cases.[61] In the absence of such training and facilities, law enforcement agents are unable to effectively prosecute cases of TNCC and this constitutes jurisdictional challenge.

Inadequate enforceable mutual assistance provisions

Inadequate enforceable mutual assistance provision with foreign States is also a problem that constitutes a jurisdictional issue for TNCCs. Even when both the host and victim states have adequate criminal statutes and investigative powers, the prosecution is frustrated by the absence of enforceable cooperation.[62]

International cooperation between criminal justice authorities is needed for several potential reasons; data is volatile and likely to be found outside the jurisdiction of the prosecuting state; supplementary forensic skill might be necessary as international cooperation is a two way street. A comprehensive and coherent international standard on cybercrime and electronic evidence is a requirement for the effective prosecution of TNCCs.[63] The absence of this presents jurisdictional challenges. Inadequate regimes of international legal assistance and extradition can shield cybercriminals from law enforcement. As France's President Jacques Chirac once stated at a G8 Cybercrime Conference in Paris, "What we need is the rule of law at an international level, a universal legal framework equal to the worldwide reach of the Internet."[64] The above jurisdictional issues are particularly evident in the context of TNCCs.

INADEQUACIES OF PRESENT LEGAL RESPONSES TO TRANSNATIONAL CYBERCRIME

Effective legal responses to TNCCs must balance the time-tested principles of state independence, sovereignty and territorial integrity, with the peculiar nature of TNCCs. This is usually not easy to achieve because TNCCs transcend states and jurisdictions and cut across borders. This creates jurisdictional issues for purely domestic legal responses to it. Essentially, a cybercriminal in this context may sit in the comfort of his home, office, café or

[61] Weber, 'The Council of Europe's Convention on Cybercrime' (n 37) 425.
[62]Council of Europe, 'Second African Forum on Cybercrime 2021' (n 46)
[63] Council of Europe, 'Second African Forum on Cybercrime 2021' (n 46)
[64] S. S. Murphy, *United States Practice in International law* (Cambridge University Press, 2002) 2.

wherever he chooses, with a desktop, laptop, tablet or phone connected to the Internet and carry out his illegal activities that would be felt thousands of kilometres away in several other countries. Jurisdictional challenges to the enforcement of cybercrime laws become painfully glaring where, upon overcoming other hurdles, such a cybercriminal though clearly identified and located, cannot be tried because the forum court lacks jurisdiction. [65]

Extradition

Most legal responses to TNCCs recognise the need for international cooperation and rely on mutual legal assistance treaties or arrangements with emphases on extradition. This is often necessary where the offender and victim are located in different places. However, extradition in the context of TNCC is fraught with challenges.

A common requirement of most extradition arrangements is double criminality which requires that the offense charged be considered criminal in both the requesting and the requested jurisdictions, usually subject to a minimum level of penalty.[66] Double criminality is sometimes referred to as dual criminality. It protects states' rights by promoting reciprocity and also safeguards individual rights by shielding the individual from unexpected and unwarranted arrest and imprisonment. Most extradition treaties require this principle to be met before extradition request can be acceded to.[67]

Extradition thus requires not only that an appropriate treaty exists between the two countries concerned but also that the conduct in question be criminalized in both the referring and the receiving states. In the case of cybercrime, this is often not the case and may become a challenge where one jurisdiction does not recognise the relevant conduct as an offence.[68] According to Smith, a significant number of states are yet to update their criminal laws to address cybercrime and most states that have done so did it in a fashion that makes

[65] Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (n 48) 2.
[66] Alun Jones and Anand Doobay, *Jones on Extradition and Mutual Assistance*, (4th edn Sweet and Maxwell, 2014) 104-106.
[67]Soma T. John, Muther F. Thomas and Brissette M. I. Heidi, 'Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?'(1997) 34 Harvard. J. Legis. 223.
[68] Goodman and Brenner, The Emerging Consensus, 5-7

extraditing cybercriminals almost impossible.[69] For example, according to a survey carried out by McConnell International in 53 countries, 33 of the countries surveyed had not yet updated their laws to address any type of computer crime. Of the remaining countries, 9 had enacted legislation to address 5 or fewer types of computer crimes and 10 had updated their laws to prosecute 6 or more of the 10 types of computer crime identified. Such disharmony in cybercrime legislation makes cooperation based on extradition unenforceable.[70]

Double criminality, however, is not a necessary requirement for international cooperation or extradition under the Council of Europe Convention on Cybercrime.[71] This has led to criticism from some.[72] Where parties require a treaty as a precondition for extradition but none is in existence, the Convention also provide the necessary legal basis for extradition[73] and parties which do not require a treaty for the purposes of extradition are to recognise the offences established as extraditable offences.[74]

In addition, the Council of Europe's Convention on Cybercrime also addresses other issues surrounding extradition such as extraditable offences by doing away with the need to renegotiate individual treaties. Article 24 of the Convention provides that the offences established under Article 2-11 of the Convention are deemed extraditable offences in any extradition treaty between or among the parties. As such, parties to the Convention undertake to include such offences in any extradition treaty concluded between or among them

As commendable as these provisions are, it has been noted that these 'mutual assistance provisions are highly diluted as countries with significant cybercrime industries like Russia

[69]Smith G. Russell. "Investigating Cybercrime: Barriers and Solutions" Being a paper presented by Association of Certified Fraud Examiners at the Pacific Rim Fraud Conference held in Sydney, Australia on the 11th of September, 2003

[70] ibid

[71] Article 24(2) of the Convention on Cybercrime

[72]See Adrian Bannon, 'Cybercrime Investigation and Prosecution- Should Ireland Ratify the Cybercrime Convention?'(2007) 3 Galway Student Law Review 127. Maurushat on the other hand disagrees with Bannon and is of the opinion that dual criminality is allowed under the Convention on Cybercrime with the exception of preservation of stored computer data. See Alana Maurushat, 'Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?'(2010) 33 UNSWLJ 472.

[73] Article 24(3) of the Convention on Cybercrime

[74] Article 24(4) of the Convention on Cybercrime. See Clough, A World of Difference, 707-708.

are not parties to the Convention.'[75] Outside the sphere of operation of the Convention on Cybercrime, double criminality is still a burden to states as they must determine not only whether the action is criminalized in both states, but also the severity of punishment in both states. Because of this difficulty, Courts in the United States have at times shown an unwillingness to submit to in-depth examinations of the differences between the United States and a foreign country's laws,[76] thus allowing extradition where the criminal laws of both countries are merely similar.[77] In general, however, when the United States seeks to reach foreign criminals, they must extradite these individuals from the nations they committed their acts. Since most treaties require some level of dual criminality, it still creates an obstacle that must be overcome when seeking jurisdiction. This issue is difficult to tackle because as noted earlier, some countries have significantly underdeveloped statutes on cybercrime.[78] Thus, it continues to constitute a jurisdictional challenge to transnational cybercrime.

In addition to the problem of meeting the double criminality principle, there are other challenges. For example, there may not even be in existence an extradition treaty or mutual legal assistance treaty between the requesting state and the state having custody of the criminal. International law does not impose a duty to extradite offenders as a result, countries where criminals are located may refuse to extradite criminals in the absence of a treaty.[79] This development presents an insurmountable challenge to the enforcement of cybercrime laws across the globe.

To address the lacuna created, some regional instrument like the Council of Europe's Convention on Cybercrime insists on cooperation in relation to transnational cybercrime

[75] Maurushat, 'Australia's Accession to the Cybercrime Convention' (n 71) 472.
[76] This is due in large part to a lack of knowledge concerning comparative law. For an example of where double criminality was completely ignored, see *United States v. Deaton,* 448 F. Supp. 532 (N.D. Ohio 1978), which states that the particular crime was so peculiar to the U.S. system that it would be unnecessary to look for a counterpart in German law. See also Jonathan O. Hafen, 'International Extradition: Issues Arising under the Dual Criminality Requiremen'*"* (1992) BYU L. REV. 191.
[77] Soma, Muther and Brissette, 'Transnational Extradition for Computer Crimes' (n 66) 317.
[78] Salil Mehra, 'Laws and Cybercrime in the United States' (2010) 58 Am J Comp Law 684.
[79] The United States Supreme Court in *Factor v. Laubenheimer* (1933) 27290 U.S. 276, 287 for example interpreted international law to mean that there is no legal right to demand extradition in the absence of a treaty and the U. S. Congress mandated in 18 U.S.C. §§ 3183-31842s that there must be a treaty or convention in order to extradite one of its own nationals. *see also U.S. v. Rauscher* (1954) 119 U.S. 407, 411

even in the absence of extradition treaties but this has not been favourable to some.[80] In the main, if there is a treaty between two states, criminals may be extradited otherwise; there is no duty to accede to such a request. Even where there is an extradition treaty between the requesting state and the requested jurisdictions, there are many exceptions to extradition processes that can make it impossible to extradite an accused for trial.[81] Thus, outside the sphere of operation of the Cybercrime Convention, extradition may be thwarted if it is not provided for in the extradition treaty.

Conflicts of Jurisdiction

Some States have laws that have extraterritorial effects.[82] Multiple assertions of jurisdiction can result in conflicts. The assumption of jurisdiction on the basis of the location in which the criminal act had effect can result in a situation where more than one state is interested in regulating the relevant conduct. Some of the states involved may feel that their interest should be given priority over others.[83] This is a positive jurisdictional conflict. This can present a thorny issue.[84] According to Ryngaert, the overlapping assertions that result from multiple states' invocation of permissive principles of jurisdiction may almost unavoidably result in international friction.[85] This is realistic given the fact that in recognition of the transnational nature of cybercrime, most states are resorting to cybercrime regulations with broad jurisdiction provisions that often times have extraterritorial application.[86]

Unfortunately, as noted by Brenner and Koops, the Cybercrime Convention does not provide good guidance on how to resolve such conflicts. It merely states that when more than one party claims jurisdiction over an alleged offence established in accordance with

[80]See Bannon, 'Cybercrime Investigation and Prosecution' (n 71) 127. Also see Maurushat, 'Australia's Accession to the Cybercrime Convention' (n 71) 472

[81] See Ajayi, 'Challenges to Enforcement of Cybercrimes Laws and Policy' (n 48) 6.

[82]A good example is the United Kingdom's Computer Misuse Act and the Serious Crime Act. Other states that have enacted cybercrime laws with extraterritorial effect are the Singapore and Malaysia, Netherlands, Belgium, Germany and Australia. See Susan W. Brenner and Bert- Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4 Journal of High Technology Crime 3-46.

[83] Hannah L. Buxbaum, "Territory, Territoriality and the Resolution of Jurisdictional Conflict' (2009) 57 Am J. Comp. Law 642 -643

[84] Adel Azzam Saqf al Hait, 'Jurisdiction in Cybercrimes: A Comparative Study' (2014) 22 Journal of Law, Policy and Globalization 75.

[85] Cedric Ryngaert, "The Concept of Jurisdiction in International Law" accessed July 18, 2018, https://unijuris.sites.uu.nl>sites>2014/1

[86] Brenner and Koops, 'Approaches to Cybercrime Jurisdiction' (n 81) 42.

the Convention, parties involved should consult with a view to determining the most appropriate jurisdiction for prosecution. Such consultations are not obligatory.[87] This shortcoming of the Cybercrime Convention is a basis for criticism as the Convention did not provide any criteria for the settlement of such disputes or conflicts.[88]

On the other hand, cybercriminal conduct may have an effect in several jurisdictions but none of the States involved may be interested or able to try the offender.[89] This is a negative jurisdictional conflict. Cybercrimes such as hacking and denial of service attacks are targeted at specific computers. While states can claim jurisdiction based on the location of the computer, the effects of the crime, or the nationality of the victim; whether they will actually do so may depend on a number of factors, such as the visibility of the crime, the amount of damage and the specific connection with the country.[90]

In the case of malicious codes and other content-related cybercrimes, the nature of the crimes is such that they do not occur at a specific place but rather at numerous places at the same time. They also are not usually targeted at specific computers, persons or countries. In such cases, if the perpetrator acts from another country that is a safe haven, a negative jurisdiction conflict may occur. This may not necessarily be because there is no basis on which to assume jurisdiction but because the state may not have sufficient interest or resources to investigate or claim jurisdiction. States with the resources to do so may not be sufficiently harmed to claim jurisdiction or may think that some other states will do so and the states that have suffered remarkable damage may not have the legal or technical capacity to assume jurisdiction.[91]

Definitional Challenges

There is a general absence of agreement regarding the content of material and the extent or degree to which specific acts should be criminalized. This is due to the fact that there is no universally acceptable definition of the concept of cybercrime. According to Zavrsnik, the

[87] ibid 44.
[88] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization' (2014) 40 Monash University Law Review 707.
[89]Hait, 'Jurisdiction in Cybercrimes' (n 83) 75-85
[90] Brenner and Koops, 'Approaches to Cybercrime Jurisdiction' (81) 40.
[91]Ibid 41.

concept of cybercrime is still a very vague notion, as there are different types of lenses used to examine it which leads to many contradictory facts about its scope.[92]

At the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Cybercrime was defined in both a narrow sense as computer crimes and in a broad sense as computer related crimes.[93] In the narrow sense, cybercrime was said to cover any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.[94] In the broad sense, it was said to refer to any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[95]

Broad definitions have the effect of extending traditional offences such as murder for example to cybercrime if the offender used a keyboard to hit and kill the victim and this would hardly be the intention of any legislation on cybercrime.[96] Whereas, defined too narrowly, what amounts to cybercrime in one state may cease to be in another.[97]

A workable definition of the term cybercrime must neither be too broad nor too narrow and formulating a generally acceptable definition for the term that would include all acts mentioned in different regional and international legal instruments on cybercrime while at the same time excluding traditional crimes that are only facilitated by using computer hardware has not been an easy task. This lack of agreement regarding the content of the material and the extent or degree to which specific acts should be criminalized as cybercrime presents yet another challenge in resolving jurisdictional issues of TNCCs.

---

[92] Ales Zavrsnik, 'Cybercrime: Definitional Challenges and Criminological Particularities' (2009) 2 Masaryk Univ. J. Law Technol. 1.

[93]10th United Nations' Congress on the Prevention of Crime and the Treatment of Offenders, 2000 A/CONF.187/10.

[94]ibid

[95] Bannon, 'Cybercrime Investigation and Prosecution' (n 71) 119.

[96] Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, 2012, p.3 available at www.itu.int-D/cyb/cybersecurity/legislation.html accessed December 26, 2016.

[97]I. J. Akhere, *Cyber Law: An Introductio*, (Ehiose, 2014) 54. An exception to this would be the provision for mutual cooperation under the Council of Europe's Convention on Cybercrime.

Coverage

According to World Internet Users and Population Statistics of 2016, over 3 billion people have access to the Internet.[98] The effect of this is that the Internet provides an unprecedented pool of potential offenders and victims which allows offences to be committed on a scale that could not have been possible otherwise.[99] In addition, modern computer systems are powerful and can be used to extend criminal activities.[100]

Cybercriminals infect computers with malicious software that allows them to take control of several systems at the same time. They can use botnets to gather information about targets or for high-level attacks. The size of a botnet can vary from a few computers to more than a million computers.[101] The increase in the number of compromised computers also increases the danger that can result as well as the scale of the resulting consequences. This aspect of cybercrime makes purely domestic or even regional legal responses to it inadequate. With just a computer and a modem, a cybercriminal can victimize individuals, businesses and organizations anywhere in the world without ever setting foot outside his or her home.[102]

Some cybercriminals may deliberately weave communications through multiple countries in order to avoid being traced. The presence of safe havens (countries with inadequate cybercrime legislation) is also a major challenge in the fight against cybercrime. The global reach of the Internet renders most legal responses to it, including advanced regional responses like the Convention on Cybercrime, limited in their relevance.

---

[98] Internet World Stats, 'Internet Usage Statistics" available at http://www.internetworldstats.com/stats.htm see also, Brahima Sanou, "ICT Facts and Figures: The World in 2015," International Telecommunications Union, available at http://www.itu.int>statistics>document.

[99] Clough, *Principles of Cybercrime* (n 11) 8.

[100] Gercke, 'Understanding Cybercrime' (n 95) 74

[101]Keizer, Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, accessed October 21, 2018, www.techweb.com/wire/172303160

[102]Chris Uwaje, "Nigeria and the Challenges of Cyber Crime –Part 4" TechTrendsng.com available at http://www.techtrendsngcom/nigeria-and-the-challenge-of-cyber-crime-part-/ last visited 06-02-2015

UCC Law Journal. Volume 3 Issue 1 Jul. 2023, pp. 119-151
DOI: 10.47963/ucclj.v3i1.1253

UNIVERSAL JURISDICTION FOR TRANSNATIONAL CYBERCRIME?

Assuming jurisdiction over transnational cybercrimes is problematic because the Internet has no geographical boundaries and a single transaction may involve the laws of several countries or jurisdictions. The situation is made worse by the fact that while the effect of cybercriminal conduct may be felt in several countries, there is no uniform international law of universal application addressing issues of criminal jurisdiction on the Internet.

As earlier noted, domestic courts administer systems of criminal law designed to provide justice for victims and due process for accused persons. States' national courts exercise jurisdiction over crimes committed in their territories and proceed against those crimes committed abroad by their nationals, or against their nationals, or against their national interests. When these and other connections are absent, States' domestic courts may nevertheless exercise jurisdiction under international law over crimes of such exceptional gravity that they affect the fundamental interests of the international community as a whole.[103]

This is done on the basis of universal jurisdiction which is based solely on the nature of the crime. Domestic courts can exercise universal jurisdiction to prosecute and punish, and thereby deter, heinous acts recognized as serious crimes under international law. When national courts exercise universal jurisdiction appropriately, in accordance with internationally recognized standards of due process, they act to vindicate not merely their own interests and values but the basic interests and values common to the international community.[104]

Therefore, although fraught with controversy, universal jurisdiction is increasingly being recognized as a means of vindicating not merely States' interests and values but also the basic interests and values common to the international community. We see this playing out in the cases of terrorism, torture, piracy and in some countries like Denmark and Germany, child pornography. However, in the case of transnational cybercrime, one has to answer the following questions: are there categories of transnational cybercrime capable of affecting the fundamental interest of the international community as a whole? Are they exceptionally

[103] Gercke, 'Understanding Cybercrime' (n 95) 74.
[104] ibid

grievous enough to be accorded a universal jurisdiction? How serious should they be for them to be so recognized?

There have been cyber-attacks in several countries across the globe, the like of which should qualify as a threat to the value and interest of the international community or capable of compromising international peace and security. Some of these attacks have been discussed earlier in this paper, others of note include the Ohio Nuclear plant disruption,[105] the attacks on the Ukraine power grid,[106] the hack of Singapore's Ministry of Defence[107] and the manipulation of the United States' 2016 presidential election.[108] These examples show that some categories of cybercrimes do indeed threaten the value and interest of the international community as a whole.

Given the seriousness of some categories of TNCCs and the possibility of even more devastating cybercriminal activities in the future, the recognition of universal jurisdiction for some categories of cybercrimes is worth considering. Universal jurisdiction will never be perfect; neither will people ever feel completely at ease with a borderless system of international criminal law. The potential for states to use universal jurisdiction prosecutions as a political tool of interstate conflict will likely remain. However, the possibility of universal jurisdiction for some categories of cybercrime should not be dismissed. Universal jurisdiction will be substantially better if informed by well-developed international standards. Some scholars suggest that since few states are willing to prosecute non-nationals for

[105] See Sean B. Hoar, "Trends n Cybercrime: The Dark Side of the Internet" *Criminal Justice* 4 (2005-2006):4 and Andrea Shalal, "IAEA Chief: Nuclear Power Plant was Disrupted by Cyber Attack" accessed August 8, 2018 http://www.reuters.com/article/us-nuclear-cyber-idUSKCN12J/.

[106] See Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" Security, accessed September 18, 2018, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-unkraine-power-grid/ BBC News, "Ukraine Power Grid was Cyber-Attack" 17, January 2017, accessed September 18, 2018 http://www.bbc.com/news/technology-38573074 and Andy Greenberg, "Crash Override: The Malware that took Down A Power Grid" Security, accessed September 18, 2018, http://www.wired.com/story/crash-override-malware.

[107]See Niranjan Arasaratnam, Adrian Fisher and Chung Yee Gui, "Singapore: Cybercrime Law Strengthened" Linklters, June 14, 2018, www.linklaters.com/en/insights/publications/tmt-news-june2017/singapore-cybercrime-law-strenghtened / and Yvette Tan, "Singapore's Ministry of Defence Suffers its First Successful Cyberattacks" accessed September 18, 2018, http://mashable.com/2017/02/28/singapore-ministry -of-defence-suffers-its-first-successful-cyber-attack/.

[108] See Eric Lipton, David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times, December 13, 2016, accessed September 18, 2018, http://www.nytimes.com/2016/12/13/us/politics/russians-hack-election-dnc.html.

atrocities committed abroad, a universal jurisdiction subject to prudential concerns will over-deter prosecutions under international law,[109] but if it appears legitimate and has integrity, states may be more likely to exercise universal jurisdiction. As a step toward this goal, it is important to narrow the gap between the theoretical application of universal norms and the variation across jurisdictions that exist in practice.[110] At present, some states already claim universal jurisdiction over a restricted number of cybercrimes. For instance, Belgium and Germany claim universal jurisdiction for child pornography.[111]

(a) Universal jurisdiction for creation and dissemination of malicious codes targeting critical infrastructure.

Given the nature of universal jurisdiction and the controversy that has trailed its use, the provision for its use in the context of TNCCs should be limited to such categories that are capable of compromising international peace and security such as attacks directed at critical infrastructure and cyber-terrorism. According to the international telecommunication union (ITU), an infrastructure is considered to be critical if its incapacity or destruction would have a debilitating impact on the defence or economic security of a state.[112] These are in particular: electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The degree of civil disturbance caused by the disruption of services by Hurricane Katrina in the United States highlights the dependence of societies on the availability of these services.[113] The malicious software "Stuxnet" underlines the emerging threat posed by Internet-based attacks focusing on critical infrastructure.[114]

The rationale for the recognition of universal jurisdiction for these categories of cybercrimes is that the growing reliance on information technology makes critical infrastructure more vulnerable to attacks.[115] This is especially so where the attack is against an interconnected

---

[109] Leila Nadya Sadat, "Redefining Universal Jurisdiction*" New England Law Review* 35 (2001):241-256
[110] Brent Wible, 'De-jeopardizing justice': Domestic Prosecutions for International Crimes and the Need for Transnational Convergence' (2002) 31 Denver Journal of International Law and Policy 266.
[111] Brenner and Koops, 'Approaches to Cybercrime Jurisdiction' (n 81) 28
[112] Gercke, 'Understanding Cybercrime' (n 95) 36.
[113] ibid 37.
[114] The malware used in the Ukraine power grid hacking has been said to be more devastating than the Stuxnet see Andy Greenberg, "Crash Override: The Malware that took Down A Power Grid" Security, accessed September 18, 2018, http://www.wired.com/story/crash-override-malware
[115] Gercke, Understanding Cybercrime, 36

system that is linked to several computers and communication networks and investigating or preventing such attacks presents unique challenges.[116] Furthermore, critical infrastructures are becoming widely recognized as a potential target for terrorist attacks. This is because they are by definition vital for a state's sustainability and stability and the dependence of critical infrastructures on ICT goes beyond the energy and nuclear industry.[117]

(b) Universal jurisdiction for cyber terrorism.

Cyberterrorism should also be among the categories of transnational cybercrimes for which a universal jurisdiction should be recognized. Cyber-terrorism is the intentional use or threat of use of electronic information systems for the perpetration of terrorist acts inspired by certain motives which could be political, ideological or religious, with the aim of causing death or serious bodily injury, serious material damage, enough to create a state of fear and to compel a government or an international organization to do or to abstain from doing a given act.[118]

Given the current trend in cybercrimes, terrorists can now remotely disrupt the information technology underlying the Internet, government computer networks, critical civilian systems such as financial networks or mass media; or telephone switching equipment. They can also use computer networks to take over machines that control traffic lights, power plants, or dams in order to cause destruction, panic and fear. At other times, cyber terrorist can destroy the banks files by using logic bombs, electromagnetic pulses or high -emission radio frequency guns. They can also block emergency communications or cut off electricity or water supply or disrupt such other critical infrastructure that could result in the most damage to life and property.[119]

In addition, cyber terrorists could remotely hijack control systems, with potentially dire consequences: such as breaching dams, colliding airplanes, hacking into a hospital computer system and changing medicine prescription to lethal dosages, identifying and

[116] ibid
[117] ibid 36 – 37.
[118] Ernest Chernukhin, 'Cybercrime: New Threat and Global Response' being a paper delivered by him as the first secretary- MFA Russia Expert Group on Cybercrime held in Vienna on the 17th -21st of January 2011.
[119] ibid

recruiting potential members of terrorist groups, collecting and transferring funds, organizing terrorist acts, inciting terrorist actions and even shutting down power grids.[120]

As bad as the present may seem, the next generation of terrorists will most likely possess more powerful and easy to use hacking tools with greater potential for cyber terrorism and they are also most likely to have greater level of knowledge, skill and malware relating to hacking. Therefore, sectors of critical infrastructure such as chemical and nuclear industry, energy, health, food, transport, water, information and communication, public and legal safety order, civil administration and space and research should come within the contemplation of universal jurisdiction.

As already noted, the rationale behind the protection of critical infrastructure arises from the fact that they are often the target of terrorist and terrorist are most likely to take advantage of the internet resources to commit cybercrime because it affords them the opportunity to instill fear and shape public opinion with only small teams and minimal funds. TNCC give cyber terrorist the added advantage of making it possible to operate from a distance, making borders and other physical barriers irrelevant when carrying out their criminal conduct. Aided by Virtual Private Network (VPN), they can effortlessly cloak their true identities and locations, choosing to remain anonymous or pretending to be someone else in order to amplify the effect of such attacks.[121]

The above is a cause for concern because the aim of terrorists is often to spread havoc and cause enough harm to generate fear, to inflict death to a large scale, to cause mass destruction or compel a government or an international organisation to do or to abstain from doing an act.[122] The potential threat of cyber terrorism and the devastation that can result is a risk that far out weight and should be considered in overcoming the fear of any possible abuse of universal jurisdiction especially where its use is provided for and regulated by a treaty.

[120] ibid.
[121] ibid
[122] ibid

UCC Law Journal. Volume 3 Issue 1 Jul. 2023, pp. 119-151
DOI: 10.47963/ucclj.v3i1.1253

CONCLUSION

The advancement of technology has brought about an increase in the severity, comprehensiveness and sophistication of incidents of cybercrime. The sources of cybercrime could include states or states sponsored attacks, terrorists, organised criminal gangs and hackers. The modern reality is that TNCC is an international borderless phenomenon with far-reaching consequences for governments, businesses and individuals. As society evolves and technology continues to advance our understanding of cybercrime must be continuously revised. The persistence, prevalence and seriousness of TNCC demand a greater response from the international community. Technology is now deeply enmeshed within the fabric of society in both domestic and international settings. Cybercriminals understand that technology is a highly effective force multiplier which can be abused to enable illicit activity, and leveraged to facilitate access to a global constituency of victims in the cyberspace. Our collective dependency on technology makes this threat extremely difficult to eliminate.

Admittedly, some countries like the United States, the United Kingdom, and Singapore amongst others have tirelessly endeavoured to ensure that their cybercrime legislations reflect current trends in the cyberspace. In the main however, the various cybercrime legislations enacted by most countries have shown states consistently applying traditional territorially based rules to online activities and refusing to accept or treat the Internet as being beyond their capability, couple with this is the absence of a global consensus on the types of conduct that constitute a cybercrime; the absence of a global consensus on the legal definition of a cybercriminal conduct and the inadequacy of most extradition and mutual legal assistance treaties does not bode well for TNCCs.

This paper has shown that the criminal jurisdiction exercised by a state can rest on territorial and extra-territorial bases. In all cases of exercise of extra-territorial jurisdiction states must establish a link with the forum state. It is only in the case of universal jurisdiction that no such link is required. Under it, states can investigate or prosecute and the courts of that state can try foreign nationals for crimes committed against foreign nationals outside the territory of the forum state, even though these crimes do not harm that state's national or interests.

The universality principle is based upon the nature of the crime, and upon the international recognition of the need to prosecute those responsible for such crimes. It has also been used for certain crimes that are of such an atrocious and dangerous nature that all states have a responsibility or a legitimate interest to take action. It is only under the principles of universal jurisdiction that international law permits any state to apply its laws to certain offences even in the absence of territorial, nationality or other accepted contacts with the offender or the victim.

However, it was shown that such exercise of jurisdiction is seldom used because of the controversies surrounding its use. Although some countries like the United Kingdom, the United States and Singapore for example assume extraterritorial jurisdiction for some categories of TNCCs, effort is made to comply with the requirement of dual criminality and such cybercriminal behaviours only come within the contemplation of their extant cybercrime laws where the act in question is criminalized by the other country or countries involved. This is in recognition of the fact that dual criminality is a requirement of most extradition and mutual legal assistance treaties. In the context of TNCC, this becomes a challenge where cybercriminals route their activities through jurisdictions that do not have similar legislations or choose these countries as their base. Even beautifully crafted regional initiative like the Council of Europe Convention on Cybercrime is limited by the global scale or nature of the Internet. Therefore, to resolve jurisdictional issues arising from such cybercriminal conduct, much more is needed.

This paper recommends a global treaty under the auspices of the United Nations Organisation with provision for a universal jurisdiction for serious categories of transnational cybercrimes, such as cyber terrorism, creation and dissemination of malicious codes targeting critical infrastructures and concludes that only in this way, will most of the jurisdictional issues of transnational cybercrime be effectively resolved.

A United Nations' Convention on Cybercrime will without fail promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively and promote, facilitate and support international cooperation and technical assistance in providing an adequate response to most jurisdictional challenges to transnational cybercrime. Especially where such a Convention provides for a regulated use of a universal jurisdiction for the categories of cybercrime.

UCC Law Journal. Volume 3 Issue 1 Jul. 2023, pp. 119-151
DOI: 10.47963/ucclj.v3i1.1253

RECOMMENDATIONS

To effectively combat TNCCs and resolve issues of jurisdiction associated with it, there should be a global treaty under the auspices of the United Nations Organization.[123]The use of universal jurisdiction for the categories of transnational cybercrimes identified above should be regulated by a global treaty under the auspices of the United Nations. Under this instrument, signatories should be obligated to apply the *aut dedere aut judicare* principle. It should become operative irrespective of whether a country has requested for the extradition of criminals or not and it should not matter whether the alleged criminal is a national or foreigner. The underlying issue should be that in so far as the criminal is within the jurisdiction of any state, the obligation to extradite or prosecute will operate. As was the case in the *Question relating to the Obligation to Prosecute or extradite*.[124]

Some international treaties have already incorporated the *aut dedere aut judicare* clause. They include: the Convention on the Prevention and Punishment of the Crime of Genocide, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 2005, The Convention for the Protection of Cultural Property in the Event of an Armed Conflict 1954, the United Nations Convention Against Corruption 2014, and Geneva Conventions.[125] When this is done, it will succeed in putting in place a universal law, that would have universal applicability with only one jurisdiction, so much that, wherever these categories of cybercrimes are committed, the perpetrator will be brought to book, irrespective of where he is located.

---

[123] Mickellea M. Tennis, 'A United Nations Convention on Cybercrime' (2020) 48 Cap U L Rev 189

[124] ICJ Report, Judgment of July 12, 2012, Para. 113. In this case, Belgium claimed that Senegal breached its obligation under the Torture Convention to prosecute or extradite Mr. Hissene Habre, the former President of the Republic of Chad, to Belgium for criminal proceedings. According to Belgium, Senegal had an obligation to exercise the universal jurisdiction provided for under article 5(2) of the Convention against Torture and Other Cruel Inhuman or Degrading Treatment or Punishment. Senegal sought to rely on the defect in its domestic law as a defence but the court held that Senegal had an obligation under the Torture Convention to prosecute or extradite Mr. Habre, that parties to the Torture Convention need not establish that their personal rights have been violated in order to establish locus standi to litigate a claiming arising there from.

[125] Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (n 48) 6.

REFERENCES

Adel Azzam Saqf al Hait, 'Jurisdiction in Cybercrimes: A Comparative Study' (2014) 22 *Journal of Law, Policy and Globalization* 75.

Adrian Bannon, 'Cybercrime Investigation and Prosecution- Should Ireland Ratify the Cybercrime Convention?'(2007) 3 *Galway Student Law Review* 127.

Alana Maurushat, 'Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?'(2010) 33 *UNSWLJ* 472.

Ales Zavrsnik, 'Cybercrime: Definitional Challenges and Criminological Particularities' (2009) 2 *Masaryk University Journal of Law and Technology* 1.

Amelia M. Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 Berkeley *Technology Law Journal* 425.

Amnesty International, *Universal Jurisdiction: The duty of States to Enact and Enforce Legislation* (AI Index, 2001).

Amos Enabulele and Bright Bazuaye, *Topics in Public International law* (Malthouse, 2019).

Alun Jones and Anand Doobay, *Jones on Extradition and Mutual Assistance*, (4th edn Sweet and Maxwell, 2014).

Brent Wible, 'De-jeopardizing justice': Domestic Prosecutions for International Crimes and the Need for Transnational Convergence' (2002) 31 *Denver Journal of International Law and Policy* 266.

Christopher C. Joyner, 'Arresting Impunity: The case for Universal Jurisdiction in Bringing War Criminals to Accountability' (2007) 59 *Law and Contemporary Problems* 153.

D. Cangemi, 'Procedural law Provisions of the Council of Europe Convention on Cybercrime' (2004) 18 *International Review Law and Computer Technology* 165.

E. F. G. Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (2016) 6 *Journal of Internet and Information System* 1.

Hannah L. Buxbaum, 'Territory, Territoriality and the Resolution of Jurisdictional Conflict' (2009) 57 Am J. Comp. Law 642.

Jim I. Akhere, *Cyber Law: An Introduction*, (Ehiose, 2014) 54.

John G. McCarthy, 'The Passive Personality Principle and Its Use in Combating International Terrorism' (1981) 13 *Fordham International Law Journal* 298.

Jonathan Clough, *Principle of Cybercrime*, (Cambridge, 2015).

Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization' (2014) 40 *Monash University Law Review* 707.

Jonathan O. Hafen, 'International Extradition: Issues Arising under the Dual Criminality Requirement' (1992) *BYU L. REV*. 191.

J. Riekkinen, 'Evidence of Cybercrime and Coercive Measures in Finland.' (2016) 13 *Digital Evidence and Electronic Signature Law Review* 49.

Kenneth C. Randall, 'Universal Jurisdiction under International law' (1988) 66 *Texas Law Review* 785.

Leila Nadya Sadat, 'Redefining Universal Jurisdiction' (2001) 35 New England Law Review 241.

Malcolm N. Shaw, *International Law* (7th edn Cambridge, 2016).

Mehmet Zülfü Öner, 'The Principle of 'Universal Jurisdiction' in International Criminal Law' (2016) 7 *Law & Justice Review* 177.

Michael P. Scharf, 'Universal Jurisdiction and the Crime of Aggression' (2012) 53 *Harvard International Law Journa*l 367.

Mickellea M. Tennis, 'A United Nations Convention on Cybercrime' (2020) 48 Cap U L Rev 189.

M. Lucchetti, *Cybercrime Legislation in Africa: Regional and International Standard* (GLACY+ - Global Action on Cybercrime Extended, April 12, 2018).

N. Kshetri, 'Cybercrime and Cyber security in Africa' (2019) 22 *Journal of Global Information Technology Management* 77.

Salil Mehra, 'Laws and Cybercrime in the United States' (2010) 58 *Am J Comp Law* 684.

Soma T. John, Muther F. Thomas and Brissette M. I. Heidi, 'Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?'(1997) *34 Harvard. J. Legis*. 223.

Susan W. Brenner and Bert- Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4 *Journal of High Technology Crime* 3.

S. S. Murphy, *United States Practice in International law* (Cambridge University Press, 2002).

Smith G. Russell. "Investigating Cybercrime: Barriers and Solutions" Being a paper presented by Association of Certified Fraud Examiners at the Pacific Rim Fraud Conference held in Sydney, Australia on the 11th of September, 2003.

U. J. Orji, 'The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability,'(2018) 12 *Masaryk University Journal of Law and Technology* 91.

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime: Draft* February 2013.

Quang Trinh, Hugh Bannister and Meg O'Brien, *The Principle of Universal Jurisdiction* (Mallesons Stephens Jaques ed Australian Red Cross, 2010) 5.

STATUTES

Council of Europe Convention of Cybercrime 2001

Computer Misuse Act 1990 (United Kingdom)

European Convention on Mutual Assistance in Criminal Matters (1959)

European Convention on Extradition, December 13, 1957 U.N.T.S. 278

Serious Crime Act 2007 (United Kingdom)

Serious Crime Act 2015 (United Kingdom)

CASE LAW

Blackmer v United States (1932) 284 U. S. 421, 438

Ex parte Pinochet (No. 3) [2000]1 AC 147, 188; 119 ILR 60

Factor v. Laubenheimer (1933) 27290 U.S. 276, 287

Holmes v Bangladesh Binani Corporation [1989] 1 AC 1112, 1137

Schooner Exchange v McFaddon (1812)7 Cranch 116

Question Relating to the Obligation to Extradite or Prosecute (Belgium v. Senegal), judgment of the ICJ, July 12, 2012

United States v. Deaton, 448 F. Supp. 532

United States v Fernandez [1974], 496 Cir. F.2d 1294.

United States v. Pizzarusso 388 F.2d 8(2d Cur.1968)

United States v. Rauscher (1954) 119 U.S. 407, 411

STATUTES

Council of Europe Convention of Cybercrime 2001

Computer Misuse Act 1990 (United Kingdom)

European Convention on Mutual Assistance in Criminal Matters (1959)

European Convention on Extradition, December 13, 1957 U.N.T.S. 278

Serious Crime Act 2007 (United Kingdom)

Serious Crime Act 2015 (United Kingdom)