Article

Assessing the Effectiveness of Extradition and the Enforcement of Extra-territorial Jurisdiction in Addressing Trans-national Cybercrimes

Phenyo Sekati
https://orcid.org/0000-0002-6365-2415
Centre for Human Rights, University of Pretoria
psekati09@gmail.com

Abstract

Cyberspace operates on a geographically borderless platform, thus often rendering national laws ineffective in regulating the impact of cyber-related activities outside South African borders. Recognising this issue, South Africa adopted the Cybercrimes Act, which permits the exercise of extra-territorial jurisdiction over trans-national cyber-related offences. The enforcement and effectiveness of extra-territorial jurisdiction and extradition law have, however, proven to be challenging and controversial in the international sphere. Issues such as internet fragmentation, contrasting municipal laws, and uncoordinated regulatory actions across state boundaries have undermined existing provisions regulating trans-national cybercrimes. These issues are furthered by the increased recognition of human rights, such as the right to privacy, which has deterred international cooperation and collaboration as states are subsequently required to subject their own citizens and entities to increased interception and scrutiny. The main thesis of this investigation is aimed at reviewing the practical implications surrounding the enforcement of extra-territorial jurisdiction and extradition law over trans-national cybercrimes. To this end, states are implored to develop both domestic and multilateral cybercrime laws and to improve existing enforcement mechanisms outlined in extradition law and mutual assistance agreements.

Keywords: Cybercrimes; trans-national; traditional crimes; international co-operation; extradition laws; mutual assistance

UNISA university of south africa PRESS
Comparative and International Law Journal of Southern Africa https://doi.org/10.25159/2522-3062/10476
https://unisapressjournals.co.za/index.php/CILSA ISSN 2522-3062 (Online), ISSN 0010-4051 (Print)
Volume 55 | Number 1 | 2022 | #10476 | 36 pages

Introduction

The principle of state sovereignty is pertinent when establishing the existence and legitimacy of a state and thus forms a fundamental part of public international law.[1] One of the more general ways in which state sovereignty is enforced is through the exercise of legislative, judicial, and executive authority within the territory of a state to the exclusion of other states.[2] This forms part of a state's jurisdiction, which encompasses the powers and functions exercised by a state within its territory. Although territoriality may be exclusive to a state when its national laws are exercised, matters concerning criminal law and the violation of human rights fall outside a state's sovereignty and thus become subject to review and the repercussions enforced under public international law.[3] South Africa, as a state party to the United Nations as well as a signatory to various international human rights treaties, accepts that extra-territorial jurisdiction can be extended over matters that implicate or affect individuals outside of a state's jurisdiction.[4] Cyberspace can facilitate traditional crimes, such as theft and fraud, as well as specialised crimes such as malware and piracy.[5] The dynamic and accessible nature of cyberspace engenders violations that affect individuals and entities on an international level.[6] International law obligates states, such as South Africa, to adopt laws that regulate activities in cyberspace, and the recently enacted Cybercrimes Act 19 of 2020 is specifically analysed insofar as it aims to regulate cybercrimes on an international level.[7]

The extra-territorial jurisdiction exercised by states is limited to matters that have a direct and substantial impact on the state exercising jurisdiction.[8] This principle thus limits the exercise of a state's jurisdiction to matters which take place on the state's territory, have adverse effects on the state, or where the action in question threatens the national security or the citizens within the state exercising jurisdiction.[9]

As a response to the growing rise in domestic and international internet-related crimes, the Convention on Cybercrime (Budapest Convention) was enacted as the first

1 UNGA, *The Scope and Application of the Principle of Universal Jurisdiction (Agenda item 86)* Sixth Committee (Legal), Sixty-fifth Session (4 October – 11 November 2010).
2 Michael Akehurst, 'Jurisdiction in International Law' (1974) 46 British Yearbook of International Law 145.
3 *SS Lotus (France v Turkey)* (Judgment) 1927 PCIJ (ser A) No. 10 paras 49–50.
4 UNGA (n 1).
5 Murdoch Watney, 'A South African Perspective on Mutual Legal Assistance and Extradition in a Globalized World' (2012) 15 PELJ 292–293.
6 Watney (n 5) 293.
7 Council of Europe European Treaty Series 185 (Convention on Cybercrime 23 Preamble, Budapest 2001).
8 Cherif Bassiouni, 'Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice' (2001) 42 Va Int'L 82.
9 Bassiouni (n 8) 139.

international treaty on cybercrimes.[10] The treaty outlines a series of powers and procedures enforceable within and between states and provides a common policy that facilitates international cooperation.[11] Further, states are encouraged to adopt legislation that addresses crimes committed in cyberspace and to employ safeguards that ensure the protection of human rights during data interception.[12]

South Africa has a significant amount of literature regarding the issues relating to cyberspace and cybersecurity, however, many of these principles have not been translated into enforceable laws, particularly within South African criminal law.[13] South African victims and perpetrators are becoming increasingly exposed and implicated in cybercrime-related matters and although many of these cases occur within the country's jurisdiction, many South Africans find themselves victims of crimes committed outside the country's territory.[14] The Cybercrimes Act, which was assented to by the National Council of Provinces on 1 July 2020, seeks to regulate the activities that violate fundamental constitutional rights and/or other procedural and substantive laws in South Africa.[15]

This article seeks to investigate the circumstances under which South Africa can enforce its extra-territorial jurisdiction over cybercrimes committed outside the state's territory. Further, these circumstances are analysed against the Cybercrimes Act insofar as it influences the jurisdictional and extradition laws adopted by state parties to the Budapest Convention, and similar treaties.

The proposed approach to this study is analytical, investigative, descriptive, and comparative. South African national law regarding cybercrimes and cyber-related activities is analysed, and compared to similar jurisprudence applicable in foreign states and is interpreted in light of existing international cybercrimes and human rights treaties and principles.

10 Council of Europe (n 7) Treaty Series No. 185 *Explanatory Report to the Convention on Cybercrime* (2001) Summary.

11 Council of Europe (n 7) Art 14(1).

12 ibid Art 15(1).

13 Chiji Ezeji, Adewale Olutola and Paul Bello, 'Cyber-Related Crime in South Africa: Extent and Perspectives of State's Role-players' (2018) 31 Southern African Journal of Criminology 94–95. For the purposes of this article, cybersecurity is defined as the use of security safeguards, best practices, and policy mechanisms to defend the use of cyberspace from cyberattacks. See Dan Craigen, Nadia Diakun-Thibault and Randy Purse, 'Defining Cybersecurity' (2014) Technology Innovation Management Review 14–15.

14 Ezeji (n 13) 99; Tim Walker and others, 'Balancing Basic FNeedoms and the need to Fight Against Cybercrime' (2021) 2021(137) ISS Peace and Security Council Report 5.

15 Preeta Bhagattjee and Aphindile Govuza, 'The Cybercrimes Act is One Step Away from Becoming Law' (*Cliffe Dekker Hofmeyer*, 7 July 2020) <https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Act-is-one-step-away-from-becoming-law.html> accessed 12 October 2020.

Threats to Cyberspace and Cybersecurity: A General Exploration of the Prevalence of Cyberattacks in South Africa

The Nature and Ambits of Cyberspace

The word 'cyber' is generally thought to have originated from the Greek verb *kybereo* which translates to actions of guiding and controlling.[16] The word was subsequently coined by the late Norbert Wiener to describe computerised control systems in the late 1940s.[17] Modern-day cybernetics operate on digitised platforms that are borderless and inter-connected.[18] Although cyberspace operates on telecommunication networks and computerised systems, these complex systems and networks have allowed for the functioning of various platforms with the transfer of information and metadata being the driving force behind each of these platforms.[19]

The presence of cyberspace and information technology is continuously growing in societies across the world with more than half of the world's population being connected to the internet, as of October 2020.[20] Lawrence Lessig presented a practical indication of the expansive nature of cyberspace when he noted that:

> While they are in that place, cyberspace, they are also here. They are at a terminal screen, eating chips, ignoring the phone. They are downstairs on the computer, late at night, while their husbands are asleep. They are at work, or at cyber cafes, or in a computer lab.[21]

The nature of cyberspace suggests that the functioning thereof as well as any interactions which take place would be borderless and limitless insofar as interactive restrictions are concerned.[22] This is, however, not the case as administrative and legal regulations have found application to cybersecurity, which is addressed through the three perspectives of legislative jurisdiction.

16 Martti Lehto, 'The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies' (2013) 3(3) IJCWT 1.

17 ibid 1.

18 Uche Mbanaso and Eman Dandaura, 'The Cyberspace: Redefining a New World' (2015) 17 IOSR Journal of Computer Engineering 17.

19 ibid 18.

20 Joseph Johnson., 'Worldwide Digital Population as of October 2020' (*Statista*, 27 January 2021) <https://www.statista.com/statistics/617136/digital-population-worldwide/> accessed 05 February 2021.

21 Lawrence Lessig, 'The Zones of Cyberspace' (1996) 48 Stanford Law Review 1403.

22 ibid 1408.

Applying the Perspectives of Legislative Jurisdiction to Cyberspace and Cybersecurity

Territorial sovereignty, which is a state's exercise of power and legal authority within its legal borders, is exercised when establishing the use and limitations of information technology.[23] Regarding the zones of cyberspace, three perspectives of legislative jurisdiction are discussed. The first is the localist perspective of legislative jurisdiction,[24] which seeks to establish a link between the information disseminated within a state's territorial borders and that contained beyond those borders.[25] The regulation of data originating from outside of these borders is thus determined by the validity and strength of the link presented.[26] In contrast, the second perspective proposes a less stringent requirement insofar as the zones of cyberspace are concerned.[27] The globalist perspective holds that all communications and uses of cyberspace are linked and co-responsive.[28] Thus, state regulation is extended to all cyberspace platforms that affect the functioning and security of platforms within their own borders.[29]

The continued growth of cyberspace and cyber-related activities have led to the observance and protection of such activities, information technology, and information communication technology under treaties and general principles of public international law.[30] Accordingly, the evolutionary approach to legislative jurisdiction has been preferred in establishing the zones of cyberspace and in controlling these zones through state regulation and the imposition of territorial borders.[31] This perspective does not establish jurisdiction solely based on physical presence and geographical borders, but rather on personal jurisdiction.[32] In this instance, authorities must consider issues regarding cyberspace and cybersecurity against existing municipal, foreign and international law to determine the adequacy and legitimacy of state regulation and the subsequent territorial restrictions imposed on certain cyberspace platforms.[33]

23 Malcolm Shaw *International Law* (6th edn, CUP 2008) 1542.
24 Lessig (n 21) 1403.
25 ibid 1404.
26 ibid.
27 ibid.
28 ibid.
29 ibid.
30 Cyrus Jabbari, 'The Application of International Law in Cyberspace' (*United Nations*, 25 October 2018) <https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/> accessed 05 February 2021.
31 Daniel Farber, 'Stretching the Margins: The Geographic Nexus in Environmental Law' (1996) 48 Stanford Law Review 1247.
32 ibid 1248–1249.
33 Lessig (n 21) 1407.

Threats to Cyberspace

Cyberspace exists and functions in two spheres, namely the digital sphere and the physical environment—and this can be observed in a global shift towards the fourth industrial revolution. Therefore, although cyberspace operates on a computerised platform, a link can be found between the digital and the physical world insofar as day-to-day interactions are concerned.[34]

Cyberspace does not operate in a vacuum and as a result, threats to cyberspace also transcend past the digital sphere and into the physical environment.[35] Threats to cyberspace are defined as malicious acts which are aimed at damaging, stealing, or disrupting digital data.[36] These acts can be classified into various categories ranging from cyberwarfare and cyber terrorism to cyber espionage, cyberactivism, and cybercrimes in general.[37] Many digital platforms provide cyber defence systems which range from anti-virus software to outsourced security services, to counter threats such as malware, hacking, and phishing. These, however, serve as preventative solutions to cyberthreats and do not provide any guidelines on how to address any cybercrimes that have been committed as well as the perpetrators.[38]

It is often assumed that most cybercrimes are facilitated by terrorists, industrial spies, hackers, and organised criminal groups. Although this might be the case, investigations have shown that many cybercrimes are also facilitated by disgruntled insiders, business competitors, and even nation-states being the source of major cyberattacks against other states.[39] The emergence of these cyberattacks poses a threat to fundamental rights such as the rights to security and privacy, thus making government and state intervention necessary through the enforcement of government legislation and state treaties.[40]

The Prevalence of Cybercrimes Affecting South Africa

The nationwide COVID-19 lockdowns have led to an increase in people working from home and individuals and businesses performing their transactions and correspondences online. Consequently, the rise in online participants and activities has resulted in the

34 Valerie Goby, 'Physical Space and Cyberspace: How Do They Interrelate? A Study of Offline and Online Social Interaction Choice in Singapore' (2003) 6(6) Cyber Psychology & Behavior 639.

35 PJ Blount, *Reprogramming the World: Cyberspace and the Geography of Global Order* (E-Relations Publishing 2019) 3.

36 Abi Tyas Tunggal, 'What is a Cyber Threat?' (*UpGuard*, 25 November 2020) <https://www.upguard.com/blog/cyber-threat> accessed 1 February 2021.

37 Martti Lehto, 'Cyberspace and Cyber Warfare' (2018) 51 Information and Communication Security 100–101.

38 Mbanaso (n 18) 20.

39 Hugh Taylor, 'What Are Cyber Threats and What to Do About Them'(*The Missing Project*, 22 January 2020 <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/> accessed 3 February 2021.

40 Blount (n 35) 5.

prevalence of cybercrimes around the world and particularly in South Africa which now, at the date of writing, has the third-highest number of cybercrime victims within its territory.[41]

A study conducted by Brett van Niekerk gave insight into the details concerning cyberattacks in South Africa.[42] The study found that upon analysing the perpetrator category of cyberattacks, thirty-one per cent of the perpetrators were identified as 'hacktivists' and twenty per cent as criminals.[43] Further, the profiles of those falling victim to hacktivists were mostly state and/or political figures with the impact of these crimes resulting in data exposure.[44] Those who facilitated cyberattacks for criminal purposes did not present a strong tendency towards any victim type and the impact of these cyberattacks mostly resulted in a loss of financial assets.[45]

The Enactment of the Cybercrimes Act and Supporting Legislation

The South African government has acknowledged the continuous expansion in cyberspace, cybersecurity, and cyber incidents that threaten to delegitimise the two.[46] Consequently, legislation surrounding data protection has grown and developed beyond the implementation of the Electronic Communications and Transactions Act (ECTA) of 2002. ECTA was the first Act in South Africa to regulate electronic communications, transactions, and transfers.[47] The enactment of this Act was subsequently followed by the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) which was promulgated in 2002; and the National Cybersecurity Policy Framework which was released in 2015.[48] The Protection of Personal Information (POPI) Act was released in 2009 and enacted in 2013 as the Protection of Personal Information Act. These formed part of the first legislative frameworks to regulate individuals' right to privacy insofar as personal information and electronic communications are concerned.[49] Lastly, in an effort to address the growing rate of cyberattacks affecting South African, the Cybercrimes Act was drafted in 2017

41 Bob Koigi, 'South Africa has Third-highest Number of Cybercrime Victims Globally, Report' (*Africa Tech*, 4 June 2020) <https://africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/> accessed 4 February 2021.

42 Dr Brett van Niekerk obtained his PhD in Philosophy and Computer Systems and is an Honourary Research Fellow in cybersecurity and information warfare at the University of KwaZulu Natal. See Brett van Niekerk, 'An Analysis of Cyber Incidents in South Africa' (2017) 20 AJIC at 113–132.

43 ibid 123.

44 ibid 125–126.

45 ibid 126.

46 ibid 114.

47 Michalsons, 'Guide to ECT Act in South Africa' (25 September 2008) <https://www.michalsons.com/blog/guide-to-the-ect-act/8>1 accessed 6 February 2021.

48 Van Niekerk (n 42) 115.

49 ibid 115; Protection of Personal Information Act 9B of 2009 Preamble; Protection of Personal Information Act 4 of 2013 Preamble.

and was enacted by the National Council of Provinces and the National Assembly on 01 July 2020 and 02 December 2020 respectively.[50]

The Cybercrimes Act was drafted to regulate the investigation and prosecution of offences that take place in cyberspace and gave authorisation to electronic communication service providers and financial institutions to assist in these investigations.[51] Notably, one of the most topical objectives sought by the Act engages with the regulation of extra-territorial cybercrime jurisdiction as well as the establishment of treaties and agreements between South Africa and other states to protect and promote cybersecurity.[52]

In addition to a state's jurisdiction over cybercrimes committed within its territory, on its territorial waters, or a ship or aircraft registered in the state, it is also vested with territorial jurisdiction over offences committed by its citizens, companies, and ordinary residents.[53] Section 24 of the Cybercrimes Act further vests South Africa with extra-territorial jurisdiction over individuals and entities where the cybercrime committed affects or intends to affect any persons or entities within its territory.[54] Altogether, this Act is in line with the Budapest Convention, which allows state parties to exercise criminal jurisdiction per its domestic laws.[55] Therefore, the Act, through its adoption of the 'effects doctrine', grants state authorities the power to prosecute non-citizens even when they are found to reside outside of South Africa's territory.[56]

The act of exercising extra-territorial jurisdiction is not absolute and cannot be made without authorisation and cooperation from the affected states.[57] Consequently, the prosecution of foreign perpetrators who have violated sections of the Cybercrimes Act cannot take place unless there is a mutual extradition agreement between South Africa and the state in which the perpetrator is a citizen, permanent resident, or ordinary resident.[58]

Public international law recognises both state sovereignty and sovereign equality—states consider their best interests and the welfare of their citizens whilst having to

50 Parliamentary Monitoring Group, 'Cybercrimes Act (B6-2017) Act History' https://pmg.org.za/Act/684/ accessed 6 February 2021.

51 Cybercrimes Act 19 2020 s 34(1).

52 ibid Preamble; NCOP Security and Justice 'ATC200617: Report of the Select Committee on Security and Justice on the Cybercrimes Act [B 6B – 2017] (National Assembly – sec 75) (introduced as Cybercrimes and Cybersecurity Act [B 6 – 2017])' 11 June 2020 <https://pmg.org.za/tabled-committee-report/4209/> accessed 6 February 2021.

53 Council of Europe (n 7) Art 22(1)(a); Permanent Court of Arbitration, Island of Palmas (*Netherlands v United States of America*), Perm. Ct. of Arbitration, 2 UN Rep Int'l Arb Awards 829 (1928) 838.

54 Cybercrimes Act (n 51) s 24(1).

55 Budapest Convention (n 53) Art 22(4).

56 Michail Vagias, *The Territorial Jurisdiction of the International Criminal Court – A Jurisdictional Rule of Reason for the ICC* (Cambridge University Press 2012) 24, 59.

57 Watney (n 5) 293.

58 ibid 293–294.

maintain treaty obligations, general principles of international law, as well as the rules of international customary law.[59] This might present an otherwise balanced approach when considering the negative obligation that states have to not interfere with each other's external affairs,[60] however, this balance is disjointed when regulating cybercrimes and overall threats to cyberspace.

Cyberspace operates on an inter-connected and borderless domain and as such,[61] cybercrimes affecting South Africans can be committed from anywhere in the world, with violations of the Cybercrimes Act occurring without the perpetrators having set foot on South African territory. The implications of this are two-fold. Firstly, sections 24(1)(a)-(c) essentially become inapplicable as many perpetrators will not be on South African territory, thus precluding prosecution in the absence of extradition.[62] Moreover, principles of personal and subject jurisdiction no longer become alternative grounds of justification with the sole reliance being on extradition laws and the cooperation that South Africa receives from foreign governments.

The principles of subjective and objective territoriality are often enforced when regulating international crimes and allow a state to exercise its jurisdiction when a crime was not committed solely within the state's territory.[63] Subjective territoriality vests a state with jurisdiction where an offence had been started within the state's territory and was completed outside of its territory, whereas objective territoriality adopts the 'effects doctrine' where states are granted jurisdiction if the offence was finalised within the state's territory.[64] When exercising extra-territorial jurisdiction over cybercrimes, the application of subjective territoriality becomes irrelevant as cybercriminals would have to act within the borders of South Africa to violate sections of the Cybercrimes Act. Further, the application of objective territoriality is also presented as an insufficient remedy as both principles are premised on the concept of territoriality.[65]

South Africa has, much like most states, adopted an evolutionary perspective to its legislative jurisdiction where the 'effects doctrine' is applied in determining when to enforce extra-territorial jurisdiction over violations of the Cybercrimes Act. However, the borderless nature of cyberspace and related cyberthreats impedes the efficacy of this approach.

59 Declaration on Principles of International Law Friendly Relations and Co-operation among States in Accordance with the Charter of The United Nations 1970 at 10.

60 ibid 7.

61 Mbanaso (n 18) 18.

62 Cybercrimes Act (n 51) s 24(1)(a)–(c).

63 John Dugard and others, *Dugard's International Law: A South African Perspective* (5th edn, Juta 2019) 216.

64 ibid.

65 Susan Brenner, 'Approaches to Cybercrime Jurisdiction' (2004) 4 Journal of High Technology Law 6.

Territorial and Jurisdictional Issues in Cyberspace: Analysing the Unique Issues Faced when Investigating and Prosecuting Cybercrimes

Cybercrimes are, by nature, more complicated than traditional crimes, as multiple natural and juristic persons can be victimised by what is often perceived as an 'invisible' perpetrator. The rapid growth in internet activity and the decentralisation of cyberspace have led to the development of various data protection laws and regulations, but these laws have not been extended to regulating the extra-territorial jurisdiction that states exercise over cybercrimes.[66]

The Cybercrimes Act exercises several forms of jurisdiction over cybercrimes. First, the subjective principle is applicable when exercising extra-territorial jurisdiction over cybercrimes as jurisdiction becomes vested with the Republic if the crime was committed within its territory or if the accused is arrested on its territory or onboard a vessel, aircraft, offshore installation, or fixed platform registered in the Republic.[67] Second, the nationality principle is similarly applied as jurisdiction is vested with the state if the accused persons/entities are South African citizens, ordinary residents, and registered entities.[68] Third and most notably, the state also vests itself with objective jurisdiction over any crimes committed in or outside of the Republic against any South African citizens, entities, or restricted computer systems registered in the state.[69] Additionally, the passive personality and universal principles are also included under the Act. This section discusses the limitations of territorial jurisdiction over cybercrimes together with the challenges presented under multilateral mutual assistance procedures.

Subjective Territoriality

Subjective territoriality is imposed when states consider the physical presence of the accused when a crime was committed. A state will, therefore, only exercise jurisdiction over an act on its territory if the criminal conduct had originated from its territory, and where the criminal will of the accused can mainly be established.[70] Although this principle has proven efficient when exercising jurisdiction over most crimes, the 'physical presence' requirement presents several difficulties when prosecuting cybercrimes.

Physical Location

Once a cybercrime and the alleged perpetrator have been identified as being outside of a state's jurisdiction, measures must be taken to effectively exercise jurisdiction over

66 *Concurrence SARL v Samsung Electronics France SAS, Amazon Services Europe Sàrl* Case C-618/15 Opinion of Advocate General Wathelet (09 November 2016) (2016) para 33.

67 Cybercrimes Act (n 51) s 24(1)(a).

68 ibid s 24(1)(b).

69 ibids 24(1)(e)–(f).

70 Jean Maillart, 'The Limits of SubjectiveTerritorial Jurisdiction in the Context of Cybercrime' (2019) 19 ERA Forum 3.

the cybercrime.[71] The first consideration when exercising extra-territorial jurisdiction is the physical location of the server where the relevant electronic data (such as the relevant webpages) is available or has been stored.[72]

The application of this position to cybercrimes is flawed in two respects. First, due to the predominance of multinational cyber companies, it is likely that electronic data detailing the commission of a cybercrime may be stored on a server located in a jurisdiction that is neither the perpetrator's nor the victim's.[73] It would therefore contravene existing jurisdictional principles to vest jurisdiction with the United States of America (USA), for example, if a perpetrator from Namibia stored stolen incorporeal intellectual property from a South African citizen on a server located or randomly assigned to a routing node in the USA.

Further, because of the multifaceted and indeterminable nature of data stored on webpages, it could also be possible that only certain (illegal) portions of data are stored on one server with other webpage data relevant to the act being stored under a different server.[74] Second, and most notably, perpetrators can easily download, upload, and transfer data to different locations across a multitude of servers and jurisdictions.[75] Thus, the enforcement of extra-territorial jurisdiction under this first consideration will only instigate a series of complexities and would also question and undermine the purpose of exercising jurisdiction over an offence.[76]

Cloud Computing and Tracing Cybercrimes

The established 'digital age' and its rapid growth have led to a great deal of communications and information being contained electronically. Consequently, significant reliance is currently placed on 'cloud computing' for data storage and protection.[77] Cloud computing is a system that facilitates the transfer of data from one service provider to another and enables users to store data on different service providers enabling access over multiple servers, networks, and electronic devices.[78]

This decentralisation of information has led to an increase in cross-border data transfers, some of which have been criminal in nature.[79] As a result, the process of determining

71 Ikenga Oraegbunam, 'Towards Containing the Jurisdictional Problems in Prosecuting Cybercrimes: Case Reviews and Responses' (2016) 7 Nnamdi Azikiwe University Journal of International Law and Jurisprudence 26.
72 Oraegbunam (n 71) 31.
73 ibid 31–32; Darrel Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 Michigan Telecommunications and Technology Law Review 79.
74 Menthe (n 73) 79–80.
75 Oraegbunam (n 71) 32.
76 Oraegbunam (n 71) 32; Menthe (n 73) 71.
77 Directorate-General for Internal Policies, 'Fighting Cyber Crimes and Protecting Privacy in the Cloud' (2012) 8.
78 Directorate-General for Internal Policies (n 77) 13.
79 Directorate-General for Internal Policies (n 77) 12.

territorial jurisdiction over cybercrimes becomes complicated and onerous, especially where information spreads beyond one jurisdiction's closed networks to another jurisdiction's network or service provider. The Cybercrimes Act mainly addresses and makes provision for traditional computer retrieval procedures where information can be stored on controlled systems such as desktops, network routers, and flash drives.[80] Further, although the Budapest Convention makes provision for trans-border access to information stored on computer data, states can only access such data subject to the voluntary consent of the authorities of the member states empowered to give this consent.[81]

Evidently, access to information processed through cloud computing is restricted as both the requesting and requested states must be member states to the Convention, and consent and authorisation must be obtained from a user who may be a private person or private service provider. Moreover, Article 32(b) of the Convention also indicates that the information itself must fall under the category of 'stored computer data' and must be accessible to the requesting state within its territory.[82] The existence and increasing use of cloud computing thus present several challenges when investigating and prosecuting extra-territorial cybercrimes as the authorities who are tasked with sourcing data must establish whether the data can be accessed, determine the source from where the data originated, and must thereafter locate the service provider or user and request their authorisation if it is determined that both parties are signatories to the Budapest Convention. This process is not only time- and resource-consuming, but also undermines the efforts of authorities as the apprehension of potentially anonymous perpetrators and the seizure of data evidence is often time-sensitive owing to the indeterminacy of cyberspace.[83]

Technical Constraints

To successfully effectuate a crime in cyberspace, one must have a certain level of technical expertise and sophistication. This is especially true considering the ever-increasing development and implementation of data-protection technology. By manipulating their geographical information and concealing their internet protocol (IP) addresses, many cybercriminals have managed to remain anonymous.[84] This, combined

80 Cybercrimes Act (n 51) s 1(1)(d) and Ch 3. The Act only makes reference to computer data service mediums, computer programs, and computer systems which are defined by data either confined to one or more computers or data which can be stored on or is physically connected to a computer. Further, no reference is made to cloud computing and the sharing of trans-border computer data.

81 Budapest Convention (n 53) Art 32.

82 ibid Art 32(b); Eleni Kyriakides, 'Critiquing DOJ's Claim that the Budapest Convention Requires the Cloud Act's Solution' (*Cross-Border Data Forum*, 09 July 2019) <https://www.crossborderdataforum.org/critiquing-dojs-claim-that-the-budapest-convention-requires-the-cloud-acts-solution/> accessed 16 August 2021.

83 Maillart (n 70) 382–383.

84 Larry Greenemeier, 'Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers' *Scientific America*, (11 June 2011) <https://www.scientificamerican.com/article/tracking-cyber-hackers/> accessed 17 August 2021.

with the legal constraints of obtaining data during criminal investigations, has become an additional constraint for authorities exercising subjective territoriality over extra-territorial cybercrimes.

As a point of departure, authorities must have some indication of the identity and location of a suspected perpetrator before a full investigation can commence. During cybercrime investigations, this information is often obtained through one's IP address—which is a unique identifier that facilitates the transfer of information to different devices on a network.[85] This identifier is used to locate the device used to facilitate a cybercrime through the public or local network that the IP address of the device was connected to.[86] As it stands, however, there is a range of software programmes that enable users to conceal their location and identity. The use of proxy servers has, for example, enabled users to hide their IP addresses by only presenting the server's address when users connect to the internet.[87] Similarly, virtual private networks (VPNs) have enabled users to conceal their geographic information by ensuring that all network traffic is sent to the primary location of the VPN as opposed to the physical location of the user.[88] Further, cybercriminals have been known to use social engineering or hacking methods to obtain the IP addresses of other persons—thereby enabling them to replace their computer systems' IP addresses with those of other persons, thus concealing the identity and geographical information of the perpetrator.[89]

The issues raised by the increased anonymity of cybercriminals are threefold. First, authorities will now require advanced technologies and other resources to identify and locate an alleged perpetrator.[90] It is common cause that the South African Police Services, as well as the National Intelligence Agency, do not have the financial and technical wherewithal to continually facilitate such investigations, especially where the alleged perpetrator is suspected to be outside the state's territory.[91] Although mutual assistance agreements may enable South Africa to collaborate with those states exercising objective territoriality over the offence in question, a certain level of investigation must be carried out by South African authorities to establish that a

85 Kaspersky 'What is an IP Address - Definition and Explanation' <https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address> accessed 17 August 2021.

86 ibid.

87 ibid.

88 Greenemeier (n 84); Kaspersky (n 85).

89 Kaspersky (n 85); Maillart (n 70) 379.

90 Allison Peters and Amy Jordan, 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime' (2020) 10(3) Journal of National Security Law and Policy 488.

91 Siyanda Dlamini and Candice Mbambo, 'Understanding Policing of Cybercrime in South Africa: The Phenomena, Challenges and Effective Responses' (2019) 5(1) Cogent Social Sciences 5–6.

cybercrime had indeed taken place, thus, leaving the state's limited expertise as a raised contention.[92]

Second, states, including South Africa, would not have the authorisation to investigate cybercrimes if there is no true indication of where the conduct took place.[93] This not only limits subjective territoriality but also affects the powers of the state should it choose to exercise extra-territorial jurisdiction over the cybercrime.

The third, and last issue pertains to the authorities' access to an alleged perpetrator's information. Service providers will often be affected by such investigations and will, therefore, be requested to grant authorisation to authorities during criminal investigations.[94] To circumvent privacy considerations, authorities often have to resort to seeking authorisation for accessing subscriber information only.[95] However, despite this data retrieval process being less invasive, the process itself and the entitlements thereunder are often not included or reflected in the domestic legislation of many states as prescribed under Article 18(1)(b) of the Budapest Convention. Notably, although this provision can be interpreted under the Protection of Personal Information Act and the Cybercrimes Act, the procedure is not extended to cybercrimes committed outside of the state's territory.

Even after states have instigated the process of investigating a trans-national cybercrime, mutual assistance procedures—especially those with signatories to the Budapest Convention—are, in themselves, onerous and time-consuming.[96] These procedures, together with the process of gaining authorisation are not only frustrating insofar as service providers are concerned, but also prolong the investigation period, thereby enabling perpetrators to flee from their current location or to impose additional measures to conceal their identities online.[97] Where perpetrators choose to move themselves or their data to another jurisdiction, the investigation process becomes

92 Peters (n 90) 499. A requesting state may only ask for assistance where the requirements and principles of bilateral extradition, such as that of dual criminality, are applicable to the requested state.

93 Peters (n 90) 515.

94 Budapest Convention (n 53) Art 14.

95 ibid Art 18(3); Maillart (n 70) 381. Subscriber information refers to a user's basic geographical and contact information such as their physical address, email address, and contact number. This information is considered to be less privacy-sensitive than content data which would otherwise give authorities access to the user's communication history. See also Council of Europe (n7) para 209.

96 Cybercrime Convention Committee, 'T-CY assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (2014) 3. Notably, response times have been recorded as being as long as 24 months.

97 Peters (n 90) 520.

lengthened as authorisation may again be required from a service provider operating from the newly located jurisdiction.[98]

The application of subjective jurisdiction will thus be useful in prosecuting perpetrators who committed crimes that fall under the Cybercrimes Act. A perpetrator would not be able to claim ignorance or argue that the act is not criminalised in their own state as subjective jurisdiction is based on territoriality, thus affording the state the power to prosecute such an individual under the Cybercrimes Act provided that the act itself meets the test of legal certainty.[99] This, however, does little to contribute to combating borderless cybercrimes in general. Therefore, although this principle is effective in establishing jurisdiction over a state's nationals or over traditional crimes in general, it does not aid in addressing cybercrimes.

Objective Territoriality and the Protective Principle

Objective territoriality is vested with a state where a crime perpetrated either in or outside a particular state had a substantial effect within the state's territory.[100] This is otherwise referred to as the 'effects principle' with the protective principle applying specifically to substantial effects of external conduct on a state's government.[101]

One of the earliest and most notable judgments which enforced the effects principle is the *Lotus* case where the Permanent Court of International Justice determined that Turkey could enforce its laws over a French citizen whose actions adversely affected the country, even though they were committed in France by a French citizen.[102] Although the collision and shipwreck of the *Boz-Kourt*, were categorised as a physical invasion,[103] the principle can similarly apply to cybercrimes, as economic devastation is also considered a valid basis upon which jurisdiction can be vested in international law.[104] This principle was similarly applied to the *Chuckleberry* case, where the US District Court determined that the state had the authority to prohibit a foreign business from making its contents accessible to US citizens through its website.[105]

98 Budapest Convention (n 53) Art 14; Cybercrime Convention Committee, 'Rules on obtaining subscriber information' (3 December 2014) <https://rm.coe.int/16802e7ad1> accessed 17 August 2021 at 122.

99 Maillart (n 70) 3.

100 John Eisinger, 'Script Kiddies Beware: The Long Arm of US Jurisdiction to Prescribe' 59(4) Washington & Lee Law Review 1520.

101 Eisinger (n 100) 1520 & 1524.

102 SS Lotus (*France v Turkey*) (Judgment) 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7) (*Lotus*) paras 30–31.

103 *Lotus* (n 102) para 14.

104 Eisinger (n 100) 1523.

105 Eisinger (n 100) 1520; *Playboy Enterprises, Inc v Chuckleberry Pub Inc.* 939 F Supp 1032 (SDNY 1996) 1033. A permanent injunction was previously issued in 1981 which prevented the defendant, Tattilo, from distributing any content related to its 'PLAYMEN' magazine to the US.

Where perpetrators commit cybercrimes affecting persons or entities within several states, consideration must be given to the laws governing such acts in all of the states involved. In 2000, a computer virus commonly known as the 'Love Bug' virus was created by Onel de Guzman, a Philippine national, and spread to the rest of the world, resulting in damages amounting to millions of dollars.[106] Although De Guzman was eventually traced by the US Federal Bureau of Investigation and the Philippines' National Bureau of Investigation, he did not face prosecution for his crimes as the Philippines had not yet had any laws or legislation criminalising computer hacking and cybercrimes in general.[107] This matter highlights the importance of states not only enacting effective cybercrime legislation to establish objective jurisdiction over a matter but also ensuring the harmonisation of cybercrime laws to facilitate more effective mutual assistance efforts between states.

Passive Personality and Universal Jurisdiction

Passive personality (or passive nationality) considers the nationality of the victim when enforcing jurisdiction and enables states to enforce their domestic laws over perpetrators outside of the state's territory. Although this theory of jurisdiction is similar to the objective and protective aspects of jurisdiction, it is the most controversial basis for establishing jurisdiction and is rarely applied, first because it assumes that all persons outside of the state's territory are aware of the laws governing the state and, second, because it assumes that the laws of foreign states are somewhat inferior in protecting both its citizens and citizens abroad.[108] In South Africa, this principle has only been accepted and applied when addressing war crimes, genocide, and crimes against humanity affecting South African citizens and residents.[109] Moreover, the enforcement of the principle in response to both felonies and misdemeanours, such as in Article 113-7 of the French Penal Code, has been criticised as violating the principles of dual criminality and comity.[110]

Universal jurisdiction extends to states where the matter concerned is of universal interest.[111] Therefore, actions must fall within the level of peremptory norms, otherwise known as *jus cogens* norms, to fall under this jurisdiction.[112] Currently, cybercrimes do

106 Susan Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4(1) Journal of High Technology Law 7.

107 ibid.

108 Oraegbunam (n 71) 61.

109 Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002 sec 4(3). This is in line with international standards as the passive personality principle is only widely applicable when addressing terrorism as well as other cruel, degrading, and inhumane treatment in accordance with the United Nations Convention Against Torture and Other Cruel, Inhumane Treatment and Punishment Preamble and Art 5.

110 Eric Cafritz and Omer Tene, 'Article 113-7 of the French Penal Code: The Passive Personality Principle' (2003) 41 Columbia Journal of Transnational Law 598.

111 Eisinger (n 100) 1533.

112 ibid; Oraegbunam (n 71) 62.

not fall under this category and although crimes such as internet piracy and the dissemination of computer viruses could fall under this, the slow development of universal jurisdiction renders this possibility unlikely for the near future.[113]

Although both of the above-mentioned principles are significant in addressing crimes against humanity and similar crimes which invoke peremptory norms, they do not aid in addressing the presented issues faced in establishing jurisdiction over extra-territorial crimes.

Key Takeaways

From this section, two major issues were raised concerning the application of extra-territorial jurisdiction over cybercrimes. The first concerns the exercise of jurisdiction where data has been stored, uploaded, or transferred through multiple servers over multiple jurisdictions, while the second concerns instances where the double criminality principle is not enforceable, thus preventing states from extraditing an accused for prosecution because the act is not recognised as a crime in the state where it was committed. In addressing these concerns, it is recommended that when all states recognise the act committed as a criminal offence, the state exercising subjective jurisdiction over the matter (based on the physical location of the perpetrator in accordance with the 'downloader/uploader theory') apply the 'dominant test' in establishing which state or states are most affected by the crime.[114] Where states are equally affected by the crime, the accused must be extradited to the first requesting state. In light of the second issue, the subjective and objective principles of jurisdiction should be considered to determine their reasonableness, appropriateness, and judicial comity.

Although the objective principle does seem to be the most effective ground upon which states can vest jurisdiction over a crime affecting their citizens, some restrictions must be considered and addressed to ensure the protection of persons and entities outside of the perpetrator's territory. To address these restrictions, it is recommended, firstly, that the Cybercrimes Act makes provision for the prosecution of cybercrimes even where the originating state does not similarly prosecute such a crime.[115] Eisinger notes that in such an instance, the enforcement of legislation must not undermine international comity, and must thus balance the interests of the affected state with those of other countries.[116] Further, these provisions must also be reasonable and prosecution by foreign states must be foreseeable—thus limiting the scope of this provision to widely-recognised cybercrimes such as cybertheft, computer hacking, and the propagation of

113 ibid.

114 Sarah Miller, 'Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention' 20(4) The European Journal of International Law 1234.

115 An example of this is noted under the US Computer Abuse Amendments Act of 1994 which prosecutes both domestic and trans-national perpetrators who facilitate and commit computer crimes against parties and entities within the state. See Eisinger (n 100) 1543.

116 Eisinger (n 100) 1538–1540.

computer viruses.[117] Second, it is recommended that the terms of use for foreign servers include disclaimers on the legality of digital data where foreign servers contain data that is criminalised under South African law, thus ensuring a level of accountability for those who use these servers to facilitate crimes recognised under the Cybercrimes Act.[118]

Although states often have several grounds upon which they can establish jurisdiction over a certain matter, several issues arise when the state exercising jurisdiction seeks to extradite the accused for the purposes of prosecuting them in the state where the effects of the crime in question were experienced. These issues become even more complicated when extradition requirements are not fulfilled. The next section analyses the enforceability of extradition laws and evaluates the effectiveness of these laws when addressing cybercrimes.

One State's Perpetrator is Another State's Protectee: Investigating how Extradition Laws Affect the Enforceability of Existing Cybercrime Legislation

State sovereignty is one of the most defining and salient principles of public international law.[119] Sovereignty rights do, however, have corresponding duties which include the duty to respect international law and cooperate with other states.[120] These duties are mainly observed and implemented to the benefit of all consenting states as they are then able to implement municipal laws that not only align with treaty and customary law obligations but are also favourable to consenting states insofar as their implementation is concerned.[121] This is, however, not the case when implementing extradition laws as the enforceability of a state's laws becomes hindered when the accused is from (and residing in) another state.[122] This issue is particularly concerning where the accused is found to have committed a cybercrime, as the physical presence of the accused is often absent or indeterminable.[123]

117 ibid.

118 This was similarly done in *Licra and UEJF v Yahoo! Inc. and Yahoo France* where the Tribunal de Grande Instance and the US Supreme Court ordered that *Yahoo!* US take all possible and relevant measures to prevent French citizens from accessing Nazi memorabilia as the exhibition of such content was in violation of Article R645-1 of the French Criminal Code. See *Yahoo! Inc., a Delaware Corporation, Plaintiff-appellee, v. La Ligue Contre Le Racisme et L'antisemitisme, a French Association; L'union Des Etudiants Juifs De France, a French Association, Defendants-appellants* 433 F 3d 1199 (9th Cir 2006).

119 Samantha Besson, 'Sovereignty' in Max Planck, *Encyclopedias of International Law* (MPEPIL 2011) para 1.

120 Besson (n 119) para 123; United Nations Charter, 24 October 1945, 1 UN Treaty Series XVI Art 2.

121 Besson (n 119) para 103.

122 Edward Wise, 'Some Problems of Extradition' (1969) 15(2) Wayne Law Review 710.

123 EFG Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (2016) 6(1) Journal of Internet and Information Systems 6.

This section analyses the nature and purpose of extradition laws as well as the circumstances under which they may be implemented. The impediments to extraditing individuals accused of committing cybercrimes are explored in light of barriers to existing laws. Finally, the solutions to these barriers are discussed with recommendations on how to strengthen the enforceability of section 23 of the Cybercrimes Act.

Extradition in International Law

Extradition in public international law is defined as 'the delivery of an accused or a convicted individual to the state where he is accused of or has been convicted of, a crime, by the state on whose territory he happens to be for the time to be.'[124] To facilitate the extradition of the accused person, the state in which the accused has committed the crime (the requesting state) will submit an extradition request to the state where the accused is a citizen or resident (the requested state).[125] Extradition requirements and laws are housed in treaty obligations where mainly bilateral and occasional multilateral agreements are reached between states.[126] This, in tandem with the sparseness of additional obligations under customary law, means that any obligations that a state has to deliver accused persons to the requesting state must be stipulated in agreements that both states have consented to.[127]

In 1990, the General Assembly adopted the Resolution for the Model Treaty on Extradition 45/116 and the Model Treaty on Mutual Assistance on Criminal Matters, 45/117.[128] This followed the Eighth UN Congress on the Prevention of Crime and Treatment of Perpetrators and is aimed at developing a guideline for states to adopt when implementing and enforcing their domestic, bilateral, and multilateral extradition laws.[129] The Commission on Crime Prevention and Criminal Justice also deployed inter-

124 Dugard (n 53) 303.

125 UN Office on Drugs and Crime Revised Manual on the Model Treaty on Extradition and on the Model Treaty on Extradition (Model Treaty on Extradition) paras 10–11.

126 Jan d'Oliveria, 'International Co-operation in Criminal Matters: The South African Contribution' (2003) 16 SACJ 324 and 361.

127 Although there are justifications for the *aut dedere aut judicare* principle receiving customary law status, the obligation to extradite and its accompanying requirements has, in itself, not had its status determined under customary law. The only exception to this is outlined in the Prevention and Punishment of the Crime of Genocide (9 December 1948) A/RES/260, Art 7, where states are obligated to grant extradition requests to requesting states where an individual or group is accused of acts of genocide. See generally Usman Hameed, '*AutDedereAutJudicare* (Extradite or Prosecute) Obligation – Whether a Duty Rooted in Customary International Law?' (2015) 5(9) International Journal of Humanities and Social Science 239–248.

128 Model Treaty on Extradition (n 125) para 2; UN Office on Drugs and Crime Revised Manual on the Model Treaty on Mutual Assistance in Criminal Matters (Model Treaty on Mutual Assistance) para 3.

129 ibid.

governmental expert groups to ensure compliance with the principles set out in the model treaties and to ensure cooperation amongst member states.[130]

The purpose of the bilateral and multilateral treaties on extradition is to ensure international cooperation and to facilitate mutual assistance mechanisms where states are faced with trans-national perpetrators.[131] Examples of multilateral treaties (applicable to South Africa) which facilitate extradition processes include Part IV of the Organisation of African Unity Convention on the Prevention and Combating of Terrorism, 1999; Article 15 of the African Union Convention on Preventing and Combating Corruption, 2003; the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988; and the International Convention for the Suppression of the Financing of Terrorism, 1999.

In reverting to a municipal context, South Africa is a party to numerous multilateral extradition and mutual legal assistance agreements. It has acceded to the European Convention on Extradition, 1957 in 2003, and has since been a party to extradition agreements with the other forty-two states that have ratified or acceded to the treaty.[132] The SADC Protocols, as well as the African Union Convention on Extradition, were signed, although they have not been entered into force.[133]

The preference in the application of bilateral agreements holds true for South Africa as it has entered into extradition agreements with fourteen states, has signed (but not yet ratified) agreements with three states, and has entered negotiations with nine states.[134] These agreements are significant as the extradition process is enforced only where an agreement exists between the states involved, thereby abiding by the principles of state sovereignty.[135]

Obligation to Extradite

The Model Treaty for Extradition outlines the duty to extradite, and this duty is also highlighted throughout various bilateral and multilateral treaties.[136] The duty or

130 ibid.

131 Model Treaty on Extradition (n 125) para 1; Model Treaty on Mutual Assistance (n 128) para 1.

132 Department of Justice and Constitutional Development, 'Extradition and Mutual Legal Assistance in criminal matters treaties' <https://www.justice.gov.za/ilr/mla.html> accessed 20 June 2021; Council of Europe, 'Chart of signatures and ratifications of Treaty 024' Status as of 2 September 2021 <https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7752573?module=signatures-by-treaty&treatynum=024> accessed 2 September 2021.

133 Department of Justice and Constitutional Development (n 132).

134 ibid.

135 *President of the Republic of South Africa and Others v Quagliani, President of the Republic of South Africa and Others v Van Rooyen and Another; Goodwin v Director-General, Department of Justice and Constitutional Development and Others* 2009 (2) SA 466 (CC) (*President of the Republic of South Africa and Others v Quagliani*) para 40; Extradition Act 67 of 1962 s 2(1)–(2).

136 UN International Law Commission, 'The obligation to extradite or prosecute (*aut dedere aut judicare*)' (2014) 2 Yearbook of the International Law Commission 4–7

obligation to extradite stems from the principle of *aut dedere aut judicare.* This principle, which means 'either extradite or prosecute' is invoked as an international effort to inhibit impunity and to ensure that states do not end up harbouring criminals.[137] This principle can be found in different forms within thirty multilateral treaties and can be read in to propose that where states are not vested with universal jurisdiction to prosecute a perpetrator, the perpetrator should be extradited to a country that is vested with jurisdiction over the matter.[138] The duty to prosecute or extradite is rooted in ensuring international order and protecting the international community's interests with security and welfare being primary considerations.[139] This principle, however, remains idealistic as many states do not consider these ideals as sufficient motivators to allocate their time and resources to ensure the effectiveness of this principle.[140] Although the *aut dedere aut judicare* principle is entrenched in thirty multilateral treaties, the lack of state practice and *opinio juris* still indicates that there is a long way to go before the principle reaches customary international law status.

State practice or *usus* requires that the specific act or practice be widespread and met with widespread acceptance.[141] This acceptance must accompany an obligatory inclination from states to ensure that the rule governing an act is continuously abided by through *opinio juris*.[142] *Usus* and *opinio juris* both require proof with such proof including the existence of a *civitas maxima* amongst states.[143] This international coordination will have to be established to prove states' sense of obligation towards the duty to extradite, and that they are willing to coordinate themselves and their resources to ensure universal mutual assistance during the extradition process.[144] As it stands, however, the obligation to prosecute or extradite is, for the most part, only considered where there are grave human rights violations, violations of international humanitarian law (eg genocide, terrorism, etcetera), and/or where there are violations of *jus cogen* norms.[145]

It is even more difficult to assume that states would adopt this obligation when the crime committed does not amount to an internationally wrongful act or a gross violation of

137 UN International Law Commission (n 136) 2; Questions relating to the Obligation to Prosecute or Extradite (*Belgium v Senegal*) (Judgment) (2012) (20 July 2012) ICJ Reports 422 paras 51 and 92.

138 Andre Ferreira and others, 'The Obligation to Extradite or Prosecute' (2013) 1 UFRGSMUN 205. Some of the multilateral treaties which include this principle are The Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, The Convention for the Protection of Cultural Property in the Event of an Armed Conflict, The UN Convention Against Corruption (United Nations Office on Drugs and Crime, 2014), and the Geneva Conventions.

139 Claire Mitchell, *Aut dedere aut judicare: The Extradite or Prosecution Clause in International Law* (Graduate Institute Publications, 2009) para 22.

140 Mitchell (n 139) para 22–23.

141 ibid para 24; Dugard (n 53) 31.

142 Dugard (n 53) 36.

143 ibid 32 and 37; Mitchell (n 139) para 21.

144 ibid.

145 *Belgium v Senegal* (n 137) para 100.

fundamental human rights. This concern is furthered in the context of cybercrimes as firstly, many cybercrimes which do not bear similarity to traditional crimes are not criminalised and secondly, it would be significantly onerous to prove that a cybercrime does give rise to the obligation to extradite under treaty or customary law if the criminal act in question is neither an extraditable offence nor an internationally wrongful act.

Grounds for Refusal Outlined in the Cybercrimes Act

The Model Treaty on Extradition outlines a list of mandatory and optional grounds for refusal. Of these grounds, specific consideration is given to the grounds of dual criminality and the *non bis in idem* rule, the speciality rule, and the evidentiary burden requirement. These grounds are considered in light of the most recent cases involving limitations similar to those outlined by the Cybercrimes Act.

Dual Criminality and *Non Bis in Indem*

The principle of dual criminality has considerable value in extradition law as it is founded on ensuring reciprocity and mutuality between states.[146] The principle entails that an accused person cannot be charged for a crime in both the requesting and sending states and is also aligned with the *maxim ne bis in idem* rule (rule against double jeopardy) which prescribes that one cannot be prosecuted more than once for the same extraditable offence.[147] Additionally, the dual criminality principle prescribes that a crime will not be considered an extraditable offence if it is not criminalised in both the requesting and sending states.[148]

Cybercrime laws and legislation are in their infancy and are still being developed in many states.[149] As a result, authorities have been presented with complexities when considering whether the requirement of dual criminality has been met in the case of a cybercrime. In *Patel v National Director of Public Prosecutions*, for example, this principle raised issues regarding the retrospective application of statutes when enforcing extradition law.[150] In this case, the United States (US) Embassy had requested that the accused, a US citizen, be extradited from South Africa to the United States of America for charges of structuring, and aiding and abetting in violation of the United States Code.[151] The applicants noted that the crime had been committed in 2005 and because South Africa had only criminalised the offence in 2010, the dual criminality requirement had not been met, thus rendering the crime a non-extraditable offence as per the two

146 *Patel v National Director of Public Prosecutions: Johannesburg* 2017 (1) SACR 456 (SCA) paras 9–10.

147 Dugard (n 53) 329; *Patel v National Director of Public Prosecutions: Johannesburg* (n 146) para 8; Ajayi (n 123) 6.

148 ibid.

149 UNCTAD, 'Cybercrime Legislation Worldwide' <https://unctad.org/page/cybercrime-legislation-worldwide> accessed 3 September 2021.

150 *Patel v National Director of Public Prosecutions: Johannesburg* (n 146).

151 ibid para 2.

states' treaty agreement.[152] The respondents, however, contended that the requested date and not the conduct date was the decisive factor when considering whether the dual criminality principle was satisfied and further argued that the applicant's considerations would only undermine mutual assistance efforts in holding accused persons accountable for crimes committed.[153] Upon analysis and consideration of the definition of an 'extraditable offence' in both the Extradition Act and the bilateral treaty between the two states, it was found that neither the treaty nor the Act[154] clarified whether the principle of dual criminality is considered at conduct or request. Article 2(1) of the treaty however indicated that an offence is only extraditable 'if it is punishable under the laws of both States by imprisonment of at least one year.' This, together with the principle of *nulla poena sine lege* affirmed that the date of conduct and not the date of request must be considered when determining whether the requirement of dual criminality had been met, as the law cannot impose retrospective criminal liability on the accused persons.[155] This consideration was also affirmed in international judgments including *R v Ex parte Pinochet Ugarte (No 3)*; and *Palazzolo v Minister of Justice and Constitutional Development & Others*.[156]

Although this determination is in line with legality principles, it does raise concerns when extraditing cybercrimes on two grounds. First, although the Cybercrimes Act has been enacted, its extra-territorial application is still largely dependent on other states criminalising similar crimes under their domestic legislation.[157] Therefore, even where South Africa has objective jurisdiction over a matter, it cannot compel another state, which may refuse to prosecute the perpetrator, to extradite its nationals if the act in question is not criminalised under its domestic law. Second, because the regulation of cybercrime is still in its developmental stages across the world, many perpetrators in states with recently enacted cybercrime legislation are able to evade prosecution, thus rendering extradition treaties ineffective if the perpetrator only committed the crime after their state's domestic legislation was enforced.[158]

Speciality Rule: Political and Military Offences

According to this principle, extradition may be refused where the offence in question is committed by a party with a political motive. The purpose of this principle is to protect those engaged in political activities from any harm or adverse control from their

152 Section 28, which criminalised the crimes in question, was only included in the Financial Intelligence Centre Act 38 of 2001 in 2010.

153 *Patel v National Director of Public Prosecutions: Johannesburg* (n 146) para 18.

154 Extradition Act (n 135) s 1; Extradition Treaty between the Government of the United States of America and the Government of the Republic of South Africa, signed at Washington on 16 September 1999 Art 2(1).

155 *Patel v National Director of Public Prosecutions: Johannesburg* (n 146) para 40.

156 See generally *Ex parte Pinochet Ugarte* (No 3) [1999] 2 WLR 824; and *Palazzolo v Minister of Justice and Constitutional Development and Others* (4731/2010) [2010] ZAWCHC 422.

157 European Convention on Extradition 13 December 1957, ETS 24 Art 7(2).

158 Ajayi (n 123) 8–9.

respective governments.[159] Notably, this provision does not extend to all politically motivated offences, especially where they are violent in nature. It is therefore important to distinguish between political and criminal offences.[160]

The scope of politically motivated offences is broad but, for the most part, includes acts such as sedition and espionage targeted against a government. Bassiouni defines 'pure' political offences as '[A] subjective threat to a political ideology or its supporting structures without any of the elements of a common crime. It is labeled a "crime" because the interest sought to be protected is the sovereign.' [161]

As the name and definition suggest, these crimes pose a direct or 'pure' threat to a state, or its government, and perpetrators will automatically be exempted from being extradited. There is a problem, however, when 'relative' political offences arise, where one or more other crimes are related to an offence that can also be construed as being politically motivated.[162] When faced with this scenario, the courts will often consider the degree of closeness between the crime(s) committed and the political motive of the said crime(s).[163] These considerations differ from state to state with varying degrees of interpretation, however—as a general test —three points of consideration are raised when determining whether a relative political offence can be exempted from extradition.[164]

The first consideration is whether the perpetrator had previously been involved in any political movements, especially where they relate to the offence committed. This is especially important in proving the subjective intention of the perpetrator as it must be determined whether the perpetrator committed the offence intending to achieve political change, thereby rendering their actions not blameworthy.[165] Second, a connection must be established between the crime(s) committed and the political objective determined by the perpetrator.[166] It, therefore, applies that if a political objective is not identified in the first step, the offence is not politically motivated, thus concluding this analysis. The final step consists of a proportionality analysis between the crime and the determined political objective to establish whether the perpetrator's prevailing interests are

159 *Quinn v Robinson,* 783 F.2d 776 (9th Cir 1986) para 806.

160 ibid.

161 Cherif Bassiouni, 'Ideologically Motivated Offenses and the Political Offenses Exception in Extradition - A Proposed Juridical Standard for an Unruly Problem' (1969) 19 DePaul Law Review 245; Charles Cantrell, 'The Political Offense Exemption in International Extradition: A Comparison of the United States, Great Britain and the Republic of Ireland' (1977) 60 Marquette Law Review 780.

162 Abraham Sofaer, 'The Political Offense Exception and Terrorism' (2020) 15(1) Denv J Int'l L & Pol'y 126.

163 *Quinn v Robinson* (n 159) para 794.

164 This test is comprised of a host of international principles that are applied with consideration to the unique circumstances faced with each 'relative' political offence.

165 *Quinn v Robinson* (n 159) para 802.

166 ibid paras 794 and 802.

politically motivated or simply rooted in criminality.[167] Although this test considers subjective elements such as the perpetrator's intention, authorities would apply an objective standard when determining whether a reasonable person in the perpetrator's position would construe their actions as political and whether the state itself would come to a similar conclusion.[168]

Although this three-step test is similarly applicable to cybercrimes, it is more difficult to first determine whether the offence is a 'pure' or 'relative' political offence and moreover, whether the perpetrator has established 'true subjective intent' should the offence be considered a 'relative political offence'.[169] For example, if a non-national were to hack into the South African government news agency's website and post defamatory statements about South Africa's head of state, calling on the nation's citizens to 'stand up against the President', it would be more arduous to determine whether the accused committed an extraditable offence as, although hacking a government's website does amount to a cybercrime against the government itself, posting such a statement together with a series of defamatory remarks against the country's head of state may be considered seditious.

It is therefore submitted that although a method to address the nature of cybercrimes could be arduous. The Cybercrimes Act has no provisions relating to politically motivated cybercrimes and the Extradition Act only leaves such a determination to the discretion of the minister.[170] Further, no current jurisprudence exists to determine whether cybercrimes committed against the state are common or political crimes, thus leaving room for perpetrators to evade extradition after having committed trans-national cybercrimes.[171]

Burden of Proof and Required Evidence

To successfully prosecute or extradite an accused individual, sufficient evidence must be collected against the individual.[172] This will often consist of 'real evidence' such as testimonies, documentation, and physical evidence.[173] Cybercrimes fall under the scope of criminal law, and the burden of proof must be beyond a reasonable doubt.[174] To satisfy this requirement, a sending state's prosecutors, as well as the receiving state's courts, will normally request a culmination of direct, circumstantial, conclusive, and/or extrinsic evidence.[175] The volume, value, and variety of evidence cannot be overstated, especially where the resources of two jurisdictional territories are used to establish the

167 ibid paras 794–796.
168 ibid para 801.
169 Ajayi (n 123) 9.
170 Extradition Act (n 135) s 15.
171 Cybercrimes Act (n 51).
172 Ajayi (n 123) 7.
173 ibid.
174 Ajayi (n 123) 7.
175 ibid.

existence of an alleged crime. This burden and requirement are particularly concerning when authorities are faced with cybercrimes, as the nature of evidence secured is often unvaried and unreliable.[176]

Although the effects of cybercrimes are often far-reaching, they are often limited to the internet and cyberspace and as a result, it is far more difficult for authorities to obtain physical evidence for such crimes than it is for physical crimes. Moreover, cybercriminals are known to only leave 'digital footprints' on accessed devices and sites and these are noted to have insufficient evidential value as they are often in the form of binary systems and algorithms that give no certain indication of the perpetrator's identity.[177] Therefore, without additional circumstantial and extrinsic evidence such as eyewitness testimonies or the accused's purchasing history, it becomes almost impossible to identify a cybercriminal.

The difficulties faced in identifying and prosecuting an accused perpetrator are exacerbated when the cybercrime has extra-territorial implications. Data stored in cyberspace is so delicate that its mere examination by an inexperienced investigator may contaminate or damage evidence resulting in increased repair and data recovery costs.[178] Added to this is the propensity of wilful destruction of evidence by cybercriminals to evade justice.[179] This results in investigators being left with little or no evidence and direction in pursuing an arrest and subsequent prosecution of such crimes.

Therefore, in addressing this requirement under extradition law, it is evident that cybercrimes present several challenges, as evidence collected in cyberspace is vulnerable to damage and manipulation, whether intentional or otherwise, which therefore renders such evidence invaluable or inadmissible by authorities and the courts during the prosecution and extradition processes.

Mutual assistance agreements have been concluded in terms of specific legislative or treaty agreements such as the South African Extradition Act and the several bilateral extradition treaties between South Africa and other member states. These agreements are, however, only effective if the crimes giving rise to extradition are uniformly outlined and criminalised. This section has highlighted how these requirements are not met when regulating cybercrimes. Thus, to ensure that perpetrators do not continuously evade prosecution or extradition, a universal set of laws should be implemented when regulating trans-national cybercrimes.[180]

176 ITU, 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (2012) 227–228.

177 Ajayi (n 123) 7.

178 Nir Kshetri, 'Cybercrime and Cybersecurity in South Africa' (2019) 22(2) Journal of Global Information Technology Management 78; Ajayi (n 123) 7.

179 ITU (n 176) 20; Ajayi (n 123) 7; Melody Musoni, 'Is Cyber Search and Seizure under the Cybercrimes and Cybersecurity Act Consistent with the Protection of the Protection of Personal Information Act?' (2016) Obiter 686.

180 Ajayi (n 123) 11.

Recommendations

Development of Cybercrime Policies and Legislation

The development of cybercrime legislation is on the rise and as of June 2021, sixty-four per cent of the United Nations' member states have been recorded to have implemented domestic legislation that criminalises computer-related offences, under the Budapest Convention. Forty-eight per cent of these states have domesticated Articles 16 to 20 of the Convention.[181] The upsurge of cybercrimes across the world has prompted a progression in laws regulating cybercrimes and the use and dissemination of data stored in cyberspace. It is, however, important that a balance is struck between enacting legislation that complies with current treaty provisions and ensuring that these laws are not overly broad to the extent that they undermine existing treaty agreements and mutual assistance procedures aimed at prosecuting and extraditing trans-national cybercrimes.[182]

Notably, the lack of uniformity, coupled with the wide disparities in the criminalisation of cybercrimes presented many restrictions for affected state authorities who wish to exercise extra-territorial jurisdiction to access data stored in cyberspace.[183] To address the substantive concerns raised throughout this paper, two recommendations are proposed.

First, a paradigm shift in the way in which states and private sector communities address and regulate cybercrimes should be prioritised and this shift should be initiated by member states to notable multilateral treaty conventions such as the Budapest Convention, the Model Treaty for Extradition, and the SADC Protocol on Extradition.[184] Traditional concepts of jurisdiction should be revisited and amended to encompass borderless crimes.

Second, cybercrimes should be considered trans-national crimes, and as such, a global multilateral treaty should be enacted which gives equal consideration to the procedural requirements for prosecuting and extraditing extra-territorial cybercrimes as it does to outlining the criminalisation of an established set of activities on cyberspace.[185] Cybercrimes consist of both cyber-dependent offences such as phishing and hacking, as well as cyber-enabled offences which would otherwise be traditional crimes, only committed in cyberspace through the use of the internet. Therefore, a governing body must make provision for both such crimes when criminalising cybercrimes.

181 Cybercrime Programme Office of the Council of Europe (C-PROC), 'Cybercrime Programme Office of the Council of Europe (C-PROC)' 2021 at 4.

182 Human Rights Watch, 'Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights' (13 August 2021) <https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights> accessed 15 September 2021.

183 ibid.

184 World Economic Forum, 'Partnership Against Cybercrime' (2020) 18.

185 Oraegbunam (n 71) 40.

To ensure that human rights are not infringed in the process of employing such measures, privacy safeguards should be employed in both instances to ensure that law enforcement does not exceed the limits of necessity and proportionality when collecting data, as this could lead to an infringement of the rights to privacy and free expression.[186]

Improvement of Current Enforcement Mechanisms

Conflicting interests regarding the use of cyberspace and varying considerations regarding individual privacy rights versus the maintenance of public order can and will most likely result in extensive negotiation, acceptance, and implementation stages when enacting a universal governing body for the regulation of cybercrimes.[187] It is therefore crucial that existing enforcement mechanisms are revisited whilst states effectively 'get their act together.' When considering existing international laws regulating prosecution and extradition as mutual assistance mechanisms, it is submitted that a way forward does not necessarily necessitate the development of new law, but rather a more efficient and cooperative implementation of existing law.

Prevention is better than cure and it is for this reason that, as a second step to addressing the surge in cybercrimes, the development of information communication technology (ICT) infrastructure should be prioritised particularly in developing states such as South Africa.[188] Additionally, deterrence mechanisms should be adopted to prevent those with advanced technological skills from pursuing criminal activities in cyberspace. Cybersecurity best practices in both the public and private sectors are also a priority.[189] Collaboration with the International Multilateral Partnership Against Cyber Threats (IMPACT) may assist in this regard as the non-governmental organisation facilitates capacity building and training particularly for developing states and does so with political neutrality.[190] It is further proposed that this initiative be enacted in regional treaties such as the Malabo Convention and the SADC Protocol.

For any of these recommendations to have relevance and applicability, greater consideration must be given to the promotion of mutual assistance agreements as well as to cooperative and collaborative efforts between states and private sector entities.[191] Although the dual criminality requirement remains an ongoing challenge, it does not impede mutual assistance endeavours.[192] Consequently, states are urged to extend their

186 Human Rights Watch (n 182).
187 ibid.
188 Adonis Palustre and David Croasdell, 'The Role of Transnational Cooperation in Cybersecurity Law Enforcement' (2019) 5602.
189 ibid.
190 ibid. IMPACT is a neutral NGO and operates alongside the United Nations and the International Telecommunications Union.
191 Human Rights Watch (n 182); World Economic Forum (n 184) 18.
192 Expert Group to Conduct a Comprehensive Study on Cybercrime 'Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020' (6–8 April 2021) 2.

collaborative efforts to data and evidence sharing.[193] To ensure the balance between public order and human rights considerations, these mutual assistance agreements should prioritise the enforcement of protection mechanisms and procedural safeguards when processing requests for access to and the collection of cross-border data.[194] Law enforcement officials should also collaborate with judiciaries from other states to ensure transparency and accountability during investigations with the assistance of private sector entities.[195] Many cybercrimes do affect private-sector entities and, as webpage owners, they often have access to technical information such as subscriber and user information.[196] This places private sector entities in an advantageous position to assist states in identifying and locating perpetrators based on their online activities.[197]

Conclusion

State sovereignty will always take centre stage because states and their citizens are vulnerable to the provisions and policies of other more powerful states. Therefore, while cyberspace may be borderless, to the advantage of perpetrators, the same cannot apply to authorities that must have proper measures in place.

This article has outlined the nature and ambit of cyberspace with reference to the effect of cybercrimes on individuals, entities, and the state. The *aut dedere, aut judicare* principle was thereafter considered, regarding the applicable grounds upon which extra-territorial jurisdiction can be vested and extradition requests accepted when prosecuting and extraditing trans-national cybercrimes. The issues that arose concerned the disparities in domestic legislation and the lack of specific regulatory mechanisms addressing cybercrimes.

In a digitalised international environment, cybercrime has seen an upsurge with cybercriminals finding it increasingly easy to avoid conviction by committing crimes in and from states where such conduct is not criminalised. Moreover, traditional theories of jurisdiction remain ineffective and inconsistent in addressing trans-national cybercrimes. To address these corollaries, priority must be given to mutual assistance agreements and the development of ICT infrastructure to ensure that the paradigm shift to having a single governing body of laws addressing and regulating cybercrimes is progressive and effective.

193 ibid.
194 Human Rights Watch (n 182); World Economic Forum (n 184) 18.
195 World Economic Forum (n 184) 18.
196 ibid.
197 ibid.

References

Ajayi EFG, ‘Challenges to Enforcement of Cyber-crimes Laws and Policy’ (2016) 6(1) Journal of Internet and Information Systems <https://doi.org/10.5897/JIIS2015.0089>

Akehurst A, ‘Jurisdiction in International Law’ (1974) 46 British Yearbook of International Law.

Bassiouni C, ‘Ideologically Motivated Offenses and the Political Offenses Exception in Extradition - A Proposed Juridical Standard for an Unruly Problem’ (1969) 19 DePaul Law Review.

Bassiouni C, ‘Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice’ (2001) 42 Virginia Journal of International Law.

Bhagattjee P, Govuza A & Sebanz S, ‘The Cybercrimes Act is One Step Away from Becoming Law’ (*Cliffe Dekker Hofmeyer*, 7 July 2020) <https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Act-is-one-step-away-from-becoming-law.htm> (accessed …

Blount PJ, Reprogramming the World: Cyberspace and the Geography of Global Order (E-International Relations, 2019).

Brenner SW and Koops BJ, ‘Approaches to Cybercrime Jurisdiction (2004) 4(1) Journal of High Technology Law.

Cafritz E and Tene O, ‘Article 113-7 of the French Penal Code: The Passive Personality Principle’ (2003) 41 Columbia Journal of Transnational Law.

Cantrell C, ‘The Political Offense Exemption in International Extradition: A Comparison of the United States, Great Britain and the Republic of Ireland’ (1977) 60 Marquette Law Review.

Council of Europe, ‘Chart of signatures and ratifications of Treaty 024’ Status as of 02 September 2021 <https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7752573?module=signatures-by-treaty&treatynum=024> (accessed

Cybercrime Convention Committee, ‘Rules on Obtaining Subscriber Information’ (Department of Justice and Constitutional Development, 3 December 2014) https://rm.coe.int/

Department of Justice and Constitutional Development, ‘Extradition and Mutual Legal Assistance in Criminal Matters Treaties’ <https://www.justice.gov.za/ilr/mla.html16802e7ad1>

Dlamini S, and Mbambo C, ‘Understanding Policing of Cyber-crime in South Africa: The Phenomena, Challenges and Effective Responses’ (2019) 5(1) Cogent Social Sciences <https://doi.org/10.1080/23311886.2019.1675404>

D'Oliveria J, 'International Co-operation in Criminal matters: The South African Contribution' (2003) 16 South African Journal of Criminal Justice.

Dugard J, Du Plessis M, Maluwa T and, Tladi D, *Dugard's International Law: A South African Perspective* (Juta 2019).

Eisinger J, 'Script Kiddies Beware: The Long Arm of U.S. Jurisdiction to Prescribe' 59(4) Washington & Lee Law Review.

Ezeji C, Olutola A, and Bello P, 'Cyber-Related Crime in South Africa: Extent and Perspectives of State's Role-players' (2018) 31 Southern African Journal of Criminology 93–110.

Farber DA, 'Stretching the Margins: The Geographic Nexus in Environmental Law' (1996) 48 Stanford Law Review <https://doi.org/10.2307/1229386>

Ferreira A and others, 'The Obligation to Extradite or Prosecute' (2013) 1 UFRGS Model United Nations Journal.

Goby V, 'Physical Space and Cyberspace: How Do They Interrelate? A Study of Offline and Online Social Interaction Choice in Singapore' (2003) 6(6) CyberPsychology & Behavior.

Greenemeier L, 'Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers' (Scientific American, 11 June 2011) <https://www.scientificamerican.com/article/tracking-cyber-hackers/>

Hameed U, 'AutDedereAutJudicare (Extradite or Prosecute) Obligation- Whether a Duty Rooted in Customary International Law?' (2015) 5(9) International Journal of Humanities and Social Science.

Human Rights Watch, 'Cybercrime is Dangerous, but a New UN Treaty could be Worse for Rights' (13 August 2021) <https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights>

Jabbari C, 'The Application of International Law in Cyberspace' (United Nations, 25 October 2018) <https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/>

Johnson J, 'Worldwide Digital Population as of October 2020' (Statista, 27 January 2021) <https://www.statista.com/statistics/617136/digital-population-worldwide/>

Kaspersky, 'What is an IP Address - Definition and Explanation' <https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address>

Keshetri N, 'Cybercrime and Cybersecurity in South Africa' (2019) 22(2) Journal of Global Information Technology Management <https://doi.org/10.1080/1097198X.2019.1603527>

Koigi B, 'South Africa has third-highest number of cybercrime victims globally, report' (Africa Tech, 4 June 2020) <https://africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/>

Kyriakides E, 'Critiquing DOJ's Claim that the Budapest Convention Requires the Cloud Act's Solution' (Cross-Border Data Forum, 9 July 2019) <https://www.crossborderdataforum.org/critiquing-dojs-claim-that-the-budapest-convention-requires-the-cloud-acts-solution/>

Lehto M, 'Cyberspace and Cyber Warfare' (2018) 51 Information and Communication Security <https://doi.org/10.4018/ijcwt.2013070101>

Lehto M, 'The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies' (2013) 3(3) International Journal of Cyber Warfare and Terrorism.

Lessig, L 'The Zones of Cyberspace' (1996) 48 Stanford Law Review <https://doi.org/10.2307/1229391>

Maillart J, 'The limits of subjective territorial jurisdiction in the context of cybercrime' (2019) 19 ERA Forum <https://doi.org/10.1007/s12027-018-0527-2>

Mbanaso UN, and Dandaura ES, 'The Cyberspace: Redefining A New World' (2015) 17 IOSR Journal of Computer Engineering.

Menthe DC, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 Michigan Telecommunications and Technology Law Review.

Michalsons, 'Guide to ECT Act in South Africa' (25 September 2008) <https://www.michalsons.com/blog/guide-to-the-ect-act/81>

Miller S, 'Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention' 20(4) The European Journal of International Law <https://doi.org/10.1093/ejil/chp078>

Mitchell C, *Aut Dedere Aut Judicare: The Extradite or Prosecution Clause in International Law* (Graduate Institute Publications, 2009) <https://doi.org/10.4000/books.iheid.249>

Musoni M, 'Is Cyber Search and Seizure under the Cybercrimes and Cybersecurity Act Consistent with the Protection of the Protection of Personal Information Act?' (2016) Obiter.

Oraegbunam I, 'Towards Containing the Jurisdictional Problems in Prosecuting Cybercrimes: Case Reviews and Responses' (2016) 7 Nnamdi Azikiwe University Journal of International Law and Jurisprudence.

Parliamentary Monitoring Group, 'Cybercrimes Act (B6-2017) Act History' <https://pmg.org.za/Act/684/>

Peters A, and Jordan A, ‘Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime’ (2020) 10(3) Journal of National Security Law and Policy.

Shaw MN, *International Law* (Cambridge University Press 2008).

Sofaer AD, ‘The Political Offense Exception and Terrorism’ (2020) 15(1) Denver Journal of International Law and Policy.

Taylor H, ‘What Are Cyber Threats and What to Do About Them’ (Prey Project, 22 January 2020) <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/>

Tunggal AT, ‘What is a Cyber Threat?’ (*UpGuard*, 25 November 2020) <https://www.upguard.com/blog/cyber-threat>

United Nations Conference on Trade and Development, ‘Cybercrime Legislation Worldwide’ <https://unctad.org/page/cybercrime-legislation-worldwide>

Van Niekerk B, ‘An Analysis of Cyber Incidents in South Africa’ (2017) 20 The African Journal of Information and Communication.

Vagias M, ‘The Territorial Jurisdiction of the International Criminal Court – A Jurisdictional Rule of Reason for the ICC’ (2012) 59 Cambridge University Press.

Watney M, ‘A South African Perspective on Mutual Legal Assistance and Extradition in a Globalized World’ (2012) 15 Potchefstroom Electronic Law Journal <https://doi.org/10.4314/pelj.v15i2.11>

Wise EM, ‘Some Problems of Extradition’ (1969) 15(2) Wayne Law Review.

International Judgments

Concurrence SARL v Samsung Electronics France SAS, Amazon Services Europe Sàrl Case C-618/15 Opinion of Advocate General Wathelet (09 November 2016) (2016)

SS Lotus (*France v Turkey*) (Judgment) 1927 PCIJ (ser A) No 10.

Permanent Court of Arbitration, Island of Palmas (*Netherlands v United States of America*), Perm.

Playboy Enterprises, Inc. Chuckleberry Pub Inc 939 F Supp 1032 (SDNY 1996) 1033Ct of Arbitration, 2 UNRep. Int’l Arb. Awards 829 (1928).

Questions relating to the Obligation to Prosecute or Extradite (*Belgium v Senegal*) (Judgment) (2012) (20 July 2012) ICJ Reports 422.

Quinn v Robinson, 783 F 2d 776 (9th Cir 1986).

Yahoo! Inc a Delaware Corporation, Plaintiff-appellee v La Ligue Contre Le Racisme et L'antisemitisme, a French Association; L'union Des Etudiants Juifs De France, a French Association, Defendants-appellants 433 F 3d 1199 (9th Cir 2006).

Legislation

Cybercrimes Act 19 of 2020.

Cybercrimes and Cybersecurity Act 2017.

Extradition Act 67 of 1962.

Financial Intelligence Centre Act 38 of 2001.

Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002.

Protection of Personal Information Act 9B of 2009.

Protection of Personal Information Act 4 of 2013.

Policy Documents

Cybercrime Programme Office of the Council of Europe (C-PROC), 'Cybercrime Programme Office of the Council of Europe (C-PROC)' (2021).

Electronic Communications Act 25 of 2002, Ch XIII.

Green Paper, 'Policy Review on Cybercrime and Cybersecurity' (2013).

Harmonization of ICT Policies in Sub-Saharan Africa, Data Protection: Southern African Development Community (SADC) Model Law (2013).

Reports

Council of Europe European Treaty Series 185 (Convention on Cybercrime 23 Preamble, Budapest 2001).

Cybercrime Convention Committee, 'T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime' (2014).

Expert Group to Conduct a Comprehensive Study on Cybercrime, 'Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020' (6–8 April 2021).

Directorate-General for Internal Policies ‘Fighting Cyber Crimes and Protecting Privacy in the Cloud’ (2012).

International Telecommunications Union ‘Understanding Cybercrime: Phenomena, Challenges and Legal Response’ (2012).

NCOP Security and Justice ‘ATC200617: Report of the Select Committee on Security and Justice on the Cybercrimes Act [B 6B – 2017] (National Assembly – sec 75) (introduced as Cybercrimes and Cybersecurity Act [B 6 – 2017])’ (11 June 2020).

Palustre A and Croasdell D, ‘The Role of Transnational Cooperation in Cybersecurity Law Enforcement’ (52nd Hawaii International Conference on System Sciences 2019) <https://doi.org/10.24251/HICSS.2019.674>

World Economic Forum, ‘Partnership Against Cybercrime’ (2020).

South African Judgments

Ex parte Pinochet Ugarte (No 3) [1999] 2 WLR 824.

Palazzolo v Minister of Justice and Constitutional Development and others (4731/2010) [2010] ZAWCHC 422.

Patel v National Director of Public Prosecutions: Johannesburg 2017 (1) SACR 456 (SCA).

President of the Republic of South Africa and Others v Quagliani; *President of the Republic of South Africa and Others v Van Rooyen and Another*; *Goodwin v Director-General, Department of Justice and Constitutional Development and others* 2009 (2) SA 466 (CC).

Treaties

Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2006).

Convention on Cybercrime (2001) 23 XI 2001 185.

Cybersecurity and Personal Data Protection (AU Convention 2014).

Declaration on Principles of International Law Friendly Relations and Co-operation among States in Accordance with the Charter of The United Nations (1970).

European Convention on Extradition (13 December 1957) ETS 24.

Extradition Treaty between the Government of the United States of America and the Government of the Republic of South Africa (signed at Washington on September 16 1999).

Prevention and Punishment of the Crime of Genocide (9 December 1948), A/RES/260.

UN Charter, 24 October 1945, 1 UN Treaty Series XVI.

UN Convention Against Torture and Other Cruel, Inhumane Treatment and Punishment.

UN Documents

UNGA, ‘The Scope and Application of the Principle of Universal jurisdiction’ (Agenda item 86) Sixth Committee (Legal) sixty-fifth session.

UN International Law Commission, ‘The Obligation to Extradite or Prosecute (Aut Dedere Aut Judicare)’ (2014) 2 Yearbook of the International Law Commission.

UN Office on Drugs and Crime Revised Manual on the Model Treaty on Extradition and on the Model Treaty on Extradition.

UN Office on Drugs and Crime Revised Manual on the Model Treaty on Mutual Assistance in Criminal Matters.