# A Comparative Critique of the *Cybercrimes Act* 19 of 2020: Positioning South Africa vis-à-vis Australia

C Lötter*

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

**Author**

Casper Lötter

**Affiliation**

North-West University, South Africa

**Email**

casperlttr@gmail.com

**Date Submitted**

16 October 2023

**Date Revised**

4 February 2025

**Date Accepted**

4 February 2025

**Date Published**

13 March 2025

**Editor**

Ms Nomthandazo Mahlangu

**Journal Editor**

Prof Wian Erlank

**How to cite this contribution**

Lötter C "A Comparative Critique of the *Cybercrimes Act* 19 of 2020: Positioning South Africa vis-à-vis Australia" *PER / PELJ* 2025(28) - DOI http://dx.doi.org/10.17159/1727-3781/2025/v28i0a17035



**DOI**
http://dx.doi.org/10.17159/1727-3781/2025/v28i0a17035

## Abstract

Proceeding from the twin premises that international cooperation is essential to fight cybercrimes effectively and that there is a need to make South African legislation more robust, I consider the provisions of the *Budapest Convention on Cybercrime* as well as the African Union's *Convention on Cyber Security and Personal Data Protection* for guidance. My methodology is poststructuralism, which is suitable for my subject matter as it allows me to even consider contradictory evidence next to uncompromised material. I am particularly interested in examining international ideas that could enhance the cyber preparedness of the South African cyber ecosystem to assess the strengths and weaknesses of South Africa's *Cybercrimes Act* in a comparative, international context, with reference to Australia. I argue that it is necessary to view the international scene regarding both the *Budapest Convention* and the African Union's Convention to situate the Australian experience in the proper perspective. Cybersecurity and awareness are, after all, a team sport. Apart from the valuable insights gained from the *Budapest Convention on Cybercrime* and the African Union's *Convention on Cyber Security and Personal Data Protection* (notably the East African experience), I find an examination of Australian policy and practice to be particularly invigorating. I find three lessons gathered from the Australian experience prudent to enhance the South African cyber environment and legislation. These are the formation of a proactive new (federal) task force (comprising one hundred of the top cyber experts in Australia) by the federal government, making payment of a ransom demand illegal, and ensuring that the retention of sensitive personal data is curtailed as much as possible (to prevent its exposure after a hack). I conclude the piece by expressing the hope that this contribution may inspire cyber criminologists to explore other profitable angles within the international frame.

## Keywords

Cybercrimes; South African regulatory framework; *Budapest Convention on Cybercrime*; the African Union's *Convention on Cyber Security and Personal Data Protection*; Australian experience; international cooperation; comparative study; proactive approach.

.....

> Everyone has skin in the game regarding Australia's cyber security. If you use the internet, have a smart device in your home, or have a perspective on what Australia's cyber security should look like, I encourage you to get involved as the Expert Advisory Board seeks views throughout the Strategy's development.[1] (Clare O'Neil, Australia's Minister for Home Affairs and Cyber Security)

# 1 Introduction

The snowballing rate of digitisation or digital transformation globally has led to businesses and governments increasingly falling victim to cyberattacks. Unless we are to revert to typewriters and paper files (which is a highly unlikely scenario for the foreseeable future), storing critical data and information on the cloud is the way to go. Cross-border banking and the digitisation of banking services (also known as online banking [apps]), for example, have greatly exposed the financial sector to huge losses because of their unpreparedness for cyberattacks[2] (essentially, crimes committed in cyberspace).[3] The Council of Europe,[4] the drafters of the *Budapest Convention* and its Protocols, defines cybercrime in terms of Title 1 (Offences against the confidentiality, integrity and availability of computer data and systems), as

> Article 2 – Illegal access
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

* Casper Lötter. PhD (UFS). Post-doctoral research fellow in the School of Philosophy North-West University, Potchefstroom Campus, South Africa. E-mail: casperlttr@gmail.com. ORCiD: https://orcid.org/0000-0001-7787-1419. This contribution is dedicated to Amanda Emmanuel, whose guidance and mentorship were instrumental in the development of my first three papers on regulatory frameworks in cyber criminology: The Social Media Bill, GILAB (General Intelligence Laws Amendment Bill) and the *Cybercrimes Act* (the focus of this paper). I am profoundly grateful for your patient and insightful guidance.

1 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf.

2 Muendo 2019 https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.

3 Snail ka Mtuze 2022 *Obiter* 540.

4 Council of Europe 2023b https://www.coe.int/en/web/cybercrime/home; Council of Europe *Convention on Cybercrime (ETS No 185)* (2001) (the *Budapest Convention*) Ch II – Measures to be taken at the national level, Section 1 – Substantive criminal law, Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems, Arts 2-8.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

    a) the production, sale, procurement for use, import, distribution or otherwise making available of:

        i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

        ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

    b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

> 3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a) ii of this article.

These statements are common cause.

Consider, for example, the inherent/cyber implications of the recent closer rapprochement between Russian president Vladimir Putin and North Korean leader Kim Jong-Un, as well as their symbolically significant face-to-face meeting on September 13, 2023, in the Russian city of Tsiolkovsky. The meeting was ostensibly arranged for Russia to obtain much-needed artillery shells for its war against Ukraine[5] but, as Robert M Dover, an expert in intelligence and national security, argues, both these countries "are highly capable cyberwar and cyber intelligence nations: they can disrupt or break key infrastructure and steal sensitive government information".[6]

The FBI[7] has identified North Korea's Lazarus Group (also known as APT38) as having been responsible for the online hacking and theft of many millions in crypto-currencies while Russia's cybercriminal group named Zarya, in tandem with their spy agency FSB, has been accused of attempting to take over critical infrastructure in the West (notably Canada, the UK and the US) by way of remote cyberattacks.[8] Oliver Dowden, the UK Cabinet Office minister, recently issued a national alert against and warned at a cyber event in Belfast against what he called "ideologically motivated, rather than financially motivated" criminal hackers.[9] "Ultimately", suggests Dover, "this deal paves the way for more dangerous technology transfers and it connects the Eastern European conflict more directly with tensions in Asia".[10]

What interests me in this contribution, however, is exploring the extent to which companies and entities comprising critical infrastructure in South Africa (Eskom, Transnet, South African National Defence Force, South African Police Services, etc)[11] are prepared or had been prepared to combat

---

5 Baker 2023 https://www.nytimes.com/2023/10/13/us/politics/north-korea-weapons-russia-ukraine.html.

6 Dover 2023 https://theconversation.com/russian-and-north-korea-artillery-deal-paves-the-way-for-dangerous-cyberwar-alliance-213583.

7 FBI 2023 https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom.

8 Sabbagh 2023 https://www.theguardian.com/technology/2023/apr/19/russian-hackers-want-to-disrupt-or-destroy-uk-infrastructure-minister-warns.

9 Sabbagh 2023 https://www.theguardian.com/technology/2023/apr/19/russian-hackers-want-to-disrupt-or-destroy-uk-infrastructure-minister-warns.

10 Dover 2023 https://theconversation.com/russian-and-north-korea-artillery-deal-paves-the-way-for-dangerous-cyberwar-alliance-213583.

11 The latter two of these government arms have both been successfully hacked, with the South African National Defence Force (SANDF) the more recent of the two. In the case of the SANDF hack, preliminary results seem to indicate that an insider

the rising threat of cybercrime in the shape of cyberattacks.[12] This is often but not always related to the concomitant threat of insider collaboration.[13] Mtuze's[14] remark, albeit in another context, that it is "useful for understanding the risks associated with the use of computers", should be understood in this context: cyberspace is here to stay for the foreseeable future and is unlikely to go away during the Information Age.

South Africa is not in good cyberspace and is more vulnerable than it could or should be. On the National Cyber Security Index (NCSI) [15] scale, which is a measure to gauge the vulnerability or otherwise of national jurisdictions against the scourge of cybercrime/attacks, South Africa ranks 59 (out of 93)[16] with a cyber-safety score (CSS) of 57.71 (on a par with Costa Rica and Bangladesh, namely other inhabitants of the Third World) for 2023, on a scale of most secure to most vulnerable. These data, however, should not be seen in isolation. I suggest that it is valuable to consider these observations in the context of South Africa's astonishing 7th place (out of a total of 193 countries, ranked from worst to least affected) on the Global Organised Crime Index[17] for 2023. In terms of its report, the Global Initiative Against Transnational Organised Crime generates a heatmap indicating that South Africa has a score of 7.18 (out of 10) and notes further that South Africa has the highest score for criminality in Southern Africa (first out of 13) and third (out of 54) in Africa.[18] This score increased from 6.63 in 2021, i.e. two years ago.

Returning to the topic of cybercrime, Singh highlights the growing menace of ransomware, which he defines as "the infiltration by malicious software of a computer or network. The aim is to limit or restrict access to critical data by encrypting files – effectively locking them – until a ransom is paid".[19] Australia appears to be making significant progress in handling demands

threat was at play. SANDF maintains it was not hacked. It claims an inside operation instead, which shows its ignorance. Goba 2023 https://www.msn.com/en-za/news/other/sandf-maintains-it-was-not-hacked-claims-it-may-be-an-inside-operation-instead/ar-AA1gazoh.

12 Singh 2021 https://theconversation.com/south-african-enterprises-cant-ignore-the-risk-of-cyber-attacks-the-threat-is-on-the-rise-166133.

13 Lötter 2023a https://mg.co.za/thoughtleader/2023-06-08-sleeping-with-the-enemy-the-rise-of-the-insider-threat-in-cybercrime/; Lötter 2023b https://mg.co.za/thought leader/2023-09-04-cybercrime-the-silent-spectre-of-insider-threats/.

14 Snail ka Mtuze 2022 *Obiter* 560.

15 NCSI 2023 https://resources.cdn.seon.io/uploads/2023/04/Cybersecurity_countries-min.pdf.

16 A position claimed by Afghanistan.

17 Global Initiative Against Transnational Organised Crime 2023 https://globalinitiative.net/analysis/ocindex-2023/.

18 Global Initiative Against Transnational Organised Crime 2023 https://globalinitiative.net/analysis/ocindex-2023/.

19 Singh 2021 https://theconversation.com/south-african-enterprises-cant-ignore-the-risk-of-cyber-attacks-the-threat-is-on-the-rise-166133.

for ransom and it is innovative strategies such as theirs that I contend could greatly enhance and fortify the South African cyber ecosystem. Bearing in mind that there is no single definition for a cyberattack, the *Electronic Communications and Transactions Act* (ECTA)[20] has defined cybercrime as

> any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems including any device or the internet or any one or more of them.[21]

In this contribution, I aim to assess the strengths and weaknesses of South Africa's *Cybercrimes Act*[22] in a comparative, international context, with particular reference to Australia. Even though the enactment of the Act was an attempt to deal exclusively and comprehensively[23] on a legislative level with cybercrime and related issues,[24] I argue that there is a need for such an assessment since cybercrime and the loss of personal data by malicious means[25] (two distinct areas of the law) have become eminently possible both because of the nature of cyberspace as well as because of the borderless landscape of the internet.[26] The globalised nature of cyberspace demands not only international cooperation but also that cyber environments urgently learn from one another. Notably in *Fourie v Van der Spuy and De Jongh Inc*[27] the court held that in a claim for damages due to a cyber hack the claimant was partially responsible for its occurrence due to a lack of diligence and an absence of cyber preparedness. Apportionment of damages was accordingly held to be in order. As such, I argue that conducting an international assessment of the *Cybercrimes Act* is essential. This assessment should include an interrogation of the lessons learned from jurisdictions that have faced similar, related or advanced issues or

---

20 *Electronic Communications and Transactions Act* 25 of 2002 (ECTA).

21 As quoted with approval by Watney "Cybercrime" 477.

22 *Cybercrimes Act* 19 of 2020.

23 By way of example, in *Okundu v S* (CA&R117/16) [2016] ZAECGHC 131 (22 November 2016) para 40, the court found it necessary to consider the fraud provision created in terms of s 86(4) of ECTA, which has now been reenacted and is equivalent to the offence stated in s 8 of the *Cybercrimes Act* 19 of 2020 (the *Cybercrimes Act*).

24 Snail ka Mtuze 2022 *Obiter* 541.

25 In this regard Snail ka Mtuze 2022 *Obiter* 539 refers to "malicious damage to property in the form of malicious code such as viruses, worms and Trojan Horses, as well as unlawful monitoring and interception of data messages". The case law set out in fn 25 of his contribution is illuminating in respect of the common law situation. The authorities he refers to include *S v Van den Berg* 1991 1 SACR 104 (T); *S v Harper* 1981 2 SA 638 (D); *S v Manuel* 1953 4 SA 523 (A) 526; and *State v Howard* (Johannesburg Regional Magistrates Court) (unreported) case number 41/258/02. Case law discussed prior to the enactment of the ECTA includes *Narlis v South African Bank of Athens* 1976 2 SA 573 (A); *R v Douvenga* (District Court of the Northern Transvaal, Pretoria) (unreported) case number 111/150/2003 of 19 August 2003; *Jafta v Ezemvelo KZN Wildlife* (D204/07) [2008] ZALC 84 (1 July 2008); and *S v Motata* (Johannesburg District Court) (unreported) case number 63/968/07.

26 Watney "Cybercrime and the investigation of cybercrime" 470–472.

27 *Fourie v Van der Spuy and De Jongh Inc* 2020 1 SA 560 (GP) para 2.

challenges. Such insights are crucial for enhancing our domestic legislation as well as the resilience of our cultural and technological framework. Australia is chosen for exploration in this contribution because of the great, innovative ideas generated by Clare O'Neil's Ministry of Home Affairs and Cyber Security, but other jurisdictions and influences are equally worthy of consideration. Other topics which immediately come to mind are the cooperation between the "quad" (Japan, Australia, the US and India), the National Institute of Standards and Technology framework generated under Obama in the United States, India's initiatives and China's,[28] which are serious attempts to make their cyberspace foolproof. To this end my methodology of choice (poststructuralism) is bound to add value.

Our complex, postmodern world demands a nuanced approach[29] to theory appropriation, and poststructuralism's inclusive "both/and" methodological approach rather than the "either/or" prioritised by traditional methodologies has the great advantage that it allows the researcher to even consider contradictory data next to unproblematic evidence.[30]

Against this background and given the need for an international perspective and a preliminary view of how vulnerable South Africa's businesses and infrastructure is, it is worth keeping in mind that the *Budapest Convention on Cybercrime* as well as the African Union's *Convention on Cyber Security and Personal Data Protection* are the two most relevant international treaties on cybercrimes and personal data protection vis-à-vis South Africa and it makes eminent sense to start the discussion by situating Australia within this ongoing, globalised debate. Beginning with an overview of the terms and objectives of these international instruments and South Africa's position in respect thereof, I proceed to consider the international scene. For this purpose I subject to scrutiny the Cyber Security Strategies of Australia intertwined with a constructive critique of the *Cybercrimes Act* (and related legislation), in the context of the insights gained from the international overview suggested. Finally, building on the insights gained from this analysis, I advance several suggestions or recommendations to enhance the effectiveness of this domestic legislative instrument before concluding the contribution with a few thoughtful takeaways.

28 Hillman *Digital Silk Road* in general.

29 Sayer 2021 https://theconversation.com/nigerian-museums-must-tell-stories-of-slavery-with-more-complexity-and-nuance-169785.

30 Olivier 2013 http://thoughtleader.co.za/bertolivier/2013/05/24/modernismpost modernism-and-poststructuralism-the-difference/.

## 2 What is South Africa's position concerning the *Budapest Convention*, facilitating international cooperation?

The question is often asked if South Africa is a signatory to the *Budapest Convention*, with the implied question of whether or not the country is actively contributing to international cooperation. The answer to this question is that the RSA is indeed a signatory to the *Budapest Convention (ETS No 185)* and its Protocols[31] and, more to the point, has been invited (together with other countries, such as Ireland, Cameroon and New Zealand) to accede, but has not yet done so.[32]

That said, I should like to suggest that, irrespective of South Africa's signatory status or its adherence to the institute's mandate, the crucial issue is whether its legislative framework enables effective contributions to international cooperation. Said differently, is the legislative framework in the RSA effective enough to combat cyberattacks given the great benefit of international cooperation this offers? On 17 November 2021, following further negotiations between the parties, the *Second Additional Protocol to the Budapest Convention on Cybercrime*[33] was opened for signature. This international conference was held in Strasbourg on 12-13 May 2021 and was devoted to the topic of enhanced international cooperation and disclosure of electronic evidence in cybercrime. The Council of Europe addresses the issue of cybercrime along the three-pronged, inter-related approach noted below:[34]

> 1) the common standards of the Convention on Cybercrime [also known as the Budapest Convention on Cybercrime, established in November 2001], together with the African Union's Convention on Cyber Security and Personal Data Protection, are the most relevant international criminal justice treaties on cybercrime and electronic evidence, [as noted above]. It is supplemented by a First Additional Protocol on Xenophobia and Racism via computer systems. A Second Additional Protocol has recently been adopted;
>
> 2) the Cybercrime Convention Committee (T-CY) consisting of representatives of the Parties to the Budapest Convention and responsible for assessing the proper implementation of the Convention, preparing Guidance Notes and additional legal instruments, and facilitating cooperation among the Parties;

---

31 Council of Europe 2023a https://coe.int/en/web/cybercrime/the-budapest-convention.

32 The reason why South Africa has not done so might be partially related to the fact that the *Budapest Convention* requires Parties to declare against xenophobia, which the South African government is apparently reluctant to do because of the political mileage domestically it has been able to extract from this abhorrent phenomenon. Lötter and Bradshaw 2022 *Acta Academica* 33-35.

33 Council of Europe *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence* (2021).

34 Council of Europe 2023b https://www.coe.int/en/web/cybercrime/home.

3) capacity building projects by the dedicated Cybercrime Programme Office of the Council of Europe (C-PROC) to assist countries worldwide to strengthen their criminal justice capacities for the investigation, prosecution and adjudication of cybercrime and other cases involving electronic evidence in line with the Convention and recommendations of the T-CY.

I should like to comment on this last observation that Australia's de-emphasis on the prosecution and punishing of cyber criminals (often harboured in enemy territory) in favour of the proactive disruption of their activities is much preferable to this great stress on criminal prosecution. South Africa, sadly, seems to have gone the Budapest rather than the Australian route. It is, of course, much easier to do damage control than to engage with cyber criminals proactively. Nevertheless, the African Union's *Convention on Cyber Security and Personal Data Protection*[35] could be "Africa's overarching policy guideline on cybercrime".[36] To assess this question intelligibly a brief overview of the terms and objectives of the *Budapest Convention*, as noted in the first objective above, is necessary. I intend to interweave this treatment with a critical discussion and assessment of the *Cybercrimes Act*.

The main objective of the treaty is "to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation".[37] By the same token I ask the question whether or not South Africa has adopted appropriate legislation "aimed at the protection of society against cybercrime", thereby promoting and encouraging international cooperation. The objective of this overview is to tease out provisions which might be of use to enhance South Africa's *Cybercrimes Act*, assuming for the moment that there is indeed a need to do so. A brief overview of the Convention insofar as it is deemed relevant to assess the Act follows.

1. Articles 2-13 of the Protocol provide for a common, minimum standard for crimes in respect of cybercriminal activity so as to promote for "this kind of harmonisation [which] alleviates the fight against such crimes on the national and on the international level as well".[38] Furthermore, this article also sets out the requirements for the international framework of "double criminality" (meaning an accused of cybercrime could be charged either in the country where the crime was committed or where the effects of the activity were felt, which need not be in the same jurisdiction). This is similar to the provision created in Article

35 African Union *Convention on Cyber Security and Personal Data Protection* (2014).

36 Muendo 2019 https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.

37 Council of Europe 2001 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

38 Council of Europe 2014 https://rm.coe.int/16800cce5b.

28(1) of the African Union's convention and protocols on cyber security.[39] The latter article also encourages the "regional harmonization of these measures". Criticism against the idea of promoting the principle of so-called "double criminality" and related ideas as embodied in this instrument is that it places too much store in the notion of reactionary strategising rather than proactive engagement, as Clare O'Neil argues in the Australian context.

2. Article 39 requires the element of criminal intent for liability (such as deriving an economic advantage from the conduct),[40] but note the observation referred to above and expressed by Oliver Dowden, the UK politician and government minister, concerning "ideologically motivated, rather than financially motivated" criminal hackers.

3. Articles 2-11 do not make provision for the criminalisation of trademark violations such as cyber-squatting.[41] The Report states that "Cyber-squatters have no intent to make active use of the domain name and seek to obtain a financial advantage by forcing the entity concerned, even though indirectly, to pay for the transfer of the ownership over the domain name. At present this conduct is considered as a trademark-related issue."[42]

4. The enumeration of offences represents "a minimum consensus not excluding extensions in domestic law". The aim of Section 1 of the Convention (Articles 2-13) is to provide a minimum forum containing prohibitive legislation to prevent or suppress computer-related crimes.

5. The Section lists five types of cyber offences. These range from offences "against the confidentiality, integrity and availability of computer data and systems" to crimes of "content", a term which relates to the unlawful production and distribution of child pornography (considered to be "one of the most dangerous *modus operandi* in recent times".)[43] Titles 2-4 relate to attacks against established legal interests which are already protected by domestic criminal law. A suggestion that the distribution of racist propaganda also be prohibited was defeated because of the concern that it might infringe on the so-called right of expression.

6. Notably, the Convention uses "technology-neutral language so that the substantive criminal law offences may be applied to both current

39 African Union *Convention on Cyber Security and Personal Data Protection* (2014).
40 Council of Europe 2014 https://rm.coe.int/16800cce5b 8.
41 Council of Europe 2014 https://rm.coe.int/16800cce5b 8.
42 Council of Europe 2014 https://rm.coe.int/16800cce5b 8.
43 Council of Europe 2014 https://rm.coe.int/16800cce5b 7.

and future technologies involved".[44] This is a great provision and ties in well with Australia's national cyber security strategy aimed at harnessing new technologies and growing "critical technology industries [such as protective cyber security technologies] and the resilience of supply chains".[45] In this respect, the Report notes the following important ideas:[46]

> The ever-expanding network of communications opens new doors for criminal activity with respect to both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. Equally, safeguards should also be adapted or developed to keep abreast of the new technological environment and new procedural powers.

7. The requirement that the conduct complained of must be done "without right" also encompasses conduct in pursuit of lawful government authority to secure public order,[47] the investigation of criminal activity or national security objectives. This is a relevant consideration given the criticism against the South African Police Service (SAPS) as the reporting authority for cyber incidents[48] in the context of their well-entrenched culture of corruption[49] and the fact that they have been successfully hacked.[50] In 2013 the SAPS was hacked by the group Anonymous and details of 16,000 whistleblowers and victims were released. The concern is certainly whether they can be trusted with such valuable information and if companies would be encouraged to confidently disclose cyber incidents to this government department.

8. Under ~~A~~rticle 2 mere access without permission is illegal as it can lead to more serious complications, as in the introduction of technical tools such as bots or cookies which are meant to retrieve information on behalf of a hacker.

9. Section 3 criminalises illegal interception[51] whereas Section 4 declares the act of data interference[52] such as the introduction of Trojan Horses

---

44 Council of Europe 2014 https://rm.coe.int/16800cce5b 7.

45 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf.

46 Council of Europe 2014 https://rm.coe.int/16800cce5b 21.

47 Perlroth *This is How They Tell Me the World Ends* 33 observes significantly that "Snowden would later say he leaked the NSA data to draw the public's attention to what he viewed as unlimited surveillance. The most troubling of his revelations seemed to be the NSA's phone call metadata collection program — a log of who called whom, when, and how long they spoke — *and the lawful interception programs that compelled companies like Microsoft and Google to secretly turn over their customer data*" (emphasis added).

48 Section 54(1) of the *Cybercrimes Act*.

49 See generally Grobler *Crossing the Line.*

50 Van Niekerk 2017 *African Journal of Information and Communication* 118.

51 Council of Europe 2014 https://rm.coe.int/16800cce5b 10-11.

52 Council of Europe 2014 https://rm.coe.int/16800cce5b 11.

or computer viruses into a system or a computer to be an illegal activity.

10. Article 6 prohibits the possession of so-called "hacker tools" also with the further aim of suppressing "the creation of a kind of black market in their production and distribution",[53] which excludes dual-use devices, thereby cementing the "subjective element of the intent of committing a computer offence".[54]

11. The ECTA creates new crimes, "Computer-related forgery" and "Computer-related fraud", to cover those situations where traditional legal interests are not adequately protected against these new forms of computer-generated "interference and attacks".[55] These provisions also feature in the *Cybercrimes Act*. As for positives regarding the promulgation of the *Cybercrimes Act*, Mtuze remarks that:[56]

> It is therefore submitted that the legislature has apparently considered the various eventualities of interference as tested by the courts and reported by law enforcement agencies, and accordingly resolved to provide a comprehensive definition for "interference" in this particular context.

An example of this is the clear, reworked and tailor-made definition of "interference" in section 5(2) and section 6(2) of the Act. Furthermore Mtuze[57] suggests that the Act has improved on the wording of the ECTA in having "cured possible deficiencies" in the latter legislation. Indeed the Act considerably extends the common law definition of guilt by providing in section 11 for an aggravated offence where the perpetrator "knows or ought reasonably to have known/suspected that the computer system is restricted". A "restricted computer system" is any data or computer system (the definition is very wide) exclusively used by any financial institution or organ of the state as encompassed by section 239 of the Constitution.[58]

12. The theft of intellectual property (literary, photographic, musical, audio-visual), notably copyright, is one of the most common cybercrimes committed. The report comments that "the ease with which unauthorised copies may be made due to digital technology and the

---

53 Council of Europe 2014 https://rm.coe.int/16800cce5b 12.
54 Council of Europe 2014 https://rm.coe.int/16800cce5b 13.
55 Council of Europe 2014 https://rm.coe.int/16800cce5b 14.
56 Snail ka Mtuze 2022 *Obiter* 549.
57 Snail ka Mtuze 2022 *Obiter* 550.
58 Section 239 of the *Constitution of the Republic of South Africa*, 1996 provides for: "'organ of state' means – (a) any department of state or administration in the national, provincial or local sphere of government; or (b) any other functionary or institution – (i) exercising a power or performing a function in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation, but does not include a court or a judicial officer."

scale of reproduction and dissemination in the context of electronic networks made it necessary to include provisions on criminal law sanctions and enhance international cooperation in this field".[59] The escalation of infringements of copyright on an international level represents one of the most widespread forms of computer-related crimes.

13. All parties to the Convention (of which South Africa is not yet one), are obliged under Paragraph 1 to create criminal offences relating to the aiding or abetting of the commission of any of the offences listed under Articles 2-10.[60] Intention to commit the offence is a prerequisite for criminal liability, which is why a service provider, as a conduit of traffic, has no duty to monitor for affected content.

14. Paragraph 4 states that corporate liability does not exclude personal liability and includes criminal, civil or administrative sanctions.[61]

15. Paragraph 1 lays down four conditions which need to be met before liability attaches to a legal person.[62] Of these, it is required that the offence was committed by a natural "person who has a leading position" and based on his/her official position within the organisation has "a power of representation or an authority to take decisions or to exercise control". Bear in mind, however, the ruling in *Fourie v Van der Spuy and De Jongh Inc,*[63] noted above, where a South African court found contributory negligence for a cyber hack on the part of the plaintiff (the victim) and apportioned damages.

16. A further offence is created under Paragraph 2, which is meant to be understood as committed by either an agent or an employee of the legal person but on condition that such was committed within the scope and duties of his/her employment or "acting under its authority". The three conditions required to ensure liability are

    (1) an offence has been committed by such an employee or agent of the legal person;

    (2) the offence has been committed for the benefit of the legal person; and

    (3) the commission of the offence has been made possible by the leading person having failed to supervise the employee or agent.[64]

17. By the same token, Article 13 makes provision for "effective, proportionate and dissuasive" sanctions for natural persons convicted

59 Council of Europe 2014 https://rm.coe.int/16800cce5b 17.
60 Council of Europe 2014 https://rm.coe.int/16800cce5b 19.
61 Council of Europe 2014 https://rm.coe.int/16800cce5b 20.
62 Council of Europe 2014 https://rm.coe.int/16800cce5b 20.
63 *Fourie v Van der Spuy and De Jongh Inc* 2020 1 SA 560 (GP).
64 Council of Europe 2014 https://rm.coe.int/16800cce5b 20.

of any of the offences created in Articles 2-11, which, in these cases, refers to incarceration where applicable.[65] The concern with this and those outlined in the previous paragraph is the emphasis on aftercare rather than proactive engagement. A shift in mindset is highly recommended.

18. Although the Convention leaves open the possibility of a Party's adopting the recommendations as to criminal procedure (Article 39, paragraph 3), Section 1 makes provision for the procedure of criminal investigation as well as the collection of evidence in electronic form.[66]

19. The challenge of identifying the perpetrator is that it requires speed and secrecy, a requirement which deviates from the usual nature traditional criminal investigation (notably the types of computer data: traffic data, content data and subscriber data) and the possible forms in which it might be encountered (stored or in the process of communication).[67]

20. Domestic law may require that certain types of data, such as personal data, held by particular types of holders must be deleted (and not retained) if the business purpose for the retention of the data has become obsolete.[68] This is a wise provision and also ties in well with the Australian requirement[69] that data not immediately necessary for use be deleted without delay. In the recommendations at the end of this contribution, I identify this aspect as a weakness in the *Cybercrimes Act*.

21. Data preservation is an important new investigative tool in addressing cybercrime, although in many jurisdictions it is a brand-new procedure in their domestic law.[70] The reasons for this are threefold. Firstly, by their very nature computer data are easily changed or deleted. Secondly, traffic data regarding past communications often contain evidence of crimes committed (such as illegal content, namely child pornography or computer viruses or other adverse instructions [Article 17]) or the commission of conventional crimes, such as fraud or drug trafficking. Thirdly, the preservation of critical evidence is obviously important for successful (criminal) prosecutions.[71]

---

65 Council of Europe 2014 https://rm.coe.int/16800cce5b 20.
66 Council of Europe 2014 https://rm.coe.int/16800cce5b 21.
67 Council of Europe 2014 https://rm.coe.int/16800cce5b 21.
68 Council of Europe 2014 https://rm.coe.int/16800cce5b 25 #154.
69 Lapham 2022 https://www.abc.net.au/news/2022-11-13/medibank-data-breach-cybersecurity-latest/101648178.
70 Council of Europe 2014 https://rm.coe.int/16800cce5b 25 #155.
71 Council of Europe 2014 https://rm.coe.int/16800cce5b 26 #155.

22. Conceivably, in appropriate circumstances, such as where the custodian of the computer data is untrustworthy, it would make better sense to seek and obtain an order for search and seizure rather than a preservation order that might be ignored.[72]

23. Paragraph 3 imposes a useful duty of confidentiality, not only to assist criminal investigation but also to secure the privacy of the person involved.[73] This provision could be very useful as far as the obligatory reporting under the *Cybercrimes Act* is concerned. If an obligation to preserve confidentially is imposed on the reporting authority (presently the SAPS), this might be a strong encouragement for victims of cyber incidents to honour the obligation to report. Anonymising cases for heuristic purposes could be a powerful idea.

24. It might be critical to examine the stored traffic data to determine their source or destination, and hence the integrity of the data is vital (Article 17).[74]

25. Since it is not known at the time of the service of the order on a particular service provider, whether or not one or more service providers are involved in the transmission of the communication, it is incumbent upon the aforementioned service provider to disclose enough of the data to enable the competent authority to "identify any other service providers and the path through which the communication was transmitted".[75]

26. The requirements for obtaining an order to search for electronic evidence are the same as those for traditional tangible evidence and must be in respect of evidence (data) that already exists and which could provide evidence of the commission of a specific crime.[76]

27. However, in the case of searching for computer data, additional measures are necessary "to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier".[77] There happen to be three reasons for this development. Firstly, the evidence (the data) is intangible. Secondly, the data need to be copied onto a disc or flash drive before they can be taken away, unlike physical, tangible evidence. The report comments that "a copy of the data remains in the computer system or storage device. Domestic law should provide for a power to make such

72 Council of Europe 2014 https://rm.coe.int/16800cce5b 27 #161.
73 Council of Europe 2014 https://rm.coe.int/16800cce5b 27 #163.
74 Council of Europe 2014 https://rm.coe.int/16800cce5b 28 #166.
75 Council of Europe 2014 https://rm.coe.int/16800cce5b 28-29 #169.
76 Council of Europe 2014 https://rm.coe.int/16800cce5b 32 #186.
77 Council of Europe 2014 https://rm.coe.int/16800cce5b 32 #187.

copies". Thirdly, because of the connectivity of computer systems, the data in question might not be stored on the specific computer system, which is addressed in the search and seizure warrant, but could well be stored and be accessible in an "associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet". For this reason, domestic law should make provision for an extension of the powers to search and seize to ensure that the criminal investigation is not redundant because it is too closely tied into the conventional criminal procedure for search and seizure of tangible evidence.

28. The existence of a wide area network or Internet within the same territory allows for the definition of a "computer system" in Article 1 to refer to "any device or a group of inter-connected or related devices" and Parties to the Convention are encouraged to empower and allow law enforcement to search and seize data along these lines, as suggested.[78] The same point applies to "the execution of a computer search [which] requires both the search of the computer system and any related computer-data storage medium (e.g., diskettes) near the computer system".[79] Due to this intimate relationship between the computer and its external storage space, paragraph 1 provides for this comprehensive legal authority.

29. Since Article 19 applies only to stored computer data, the question arises whether or not an unopened email counts as stored computer data or data in transit (also known as data in transfer). If the latter, the power of interception rather than search and seizure should apply and in this respect parties to the Convention are advised to consider how their domestic law needs to be adjusted to accommodate this anomaly.[80] In the case of South African criminal law, procedure and evidence must pass constitutional muster to be considered valid and enforceable, which is an important consideration and will be reconsidered in the context of South Africa's *Cybercrimes Act*. In this regard Mtuze[81] makes a useful if often unappreciated distinction between the commission of cybercrime, on the one hand, and the protection and regulation of data protection. In the apt words of Australia's Federal Police Commissioner, Reece Kershaw, "personal information is being used as currency".[82] As the ECTA has now been superseded by the Cybercrimes Act, Mtuze remarks that "[i]n its place,

78 Council of Europe 2014 https://rm.coe.int/16800cce5b 32 #188.
79 Council of Europe 2014 https://rm.coe.int/16800cce5b 32 #189.
80 Council of Europe 2014 https://rm.coe.int/16800cce5b 32 #190.
81 Snail ka Mtuze 2022 *Obiter* 543.
82 Judd and Walker 2022 https://www.abc.net.au/news/2022-11-11/afp-reveal-more-information-on-medibank-hacker/101643794.

the Cybercrimes Act is now the key legislation that creates offences and penalties for cybercriminality".[83]

30. The same considerations apply to the maintenance of the "integrity of the data" or maintaining the "chain of custody" of the data to avoid these pieces of evidence from being ruled inadmissible.[84]

31. The important distinction between the search of stored data and the interception of flowing data (which may be surreptitious [Articles 20 and 21]), raises the issue of notification to interested parties and its settlement is left up to the drafters of domestic law.[85]

32. Content data is distinguished from traffic data in that the latter refers to the information generated by the chain of communication (origin, size, destination, route, time, date, etc).[86] Similarly, where a service provider is absent or unable to record or collect the data, law enforcement should be able to do so themselves.[87] That said, it is of course an open question how members of the SAPS will manage higher grade work if many of these persons struggle to complete an affidavit. I suggest that this consideration motivates the assignment of a specialised task force filled with experts on cybercrimes, as the Australian experience shows.

33. With many computer crimes, the transmission or communication of data is an integral part of the commission of the offence, such as the distribution of viruses or child pornography.[88]

34. Article 22 creates a range of criteria to establish obligatory jurisdiction over offences enumerated under Articles 2-11 of the Convention as the commission of a cybercrime or hack could affect many victims in many different countries.[89] Once again, as I note below, the Australian experience provides valuable guidance on this point in its absolute prohibition of the payment of ransom for hacked data, but robust international cooperation is of course necessary to ensure this initiative's effectiveness. International cooperation is after all a team sport.

35. There will be occasions where more than one Party has jurisdiction over many or all of the accused and in cases such as these "[i]n order to avoid duplication of effort, unnecessary inconvenience for

---

83 Snail ka Mtuze 2022 *Obiter* 545.
84 Council of Europe 2014 https://rm.coe.int/16800cce5b 33 #197.
85 Council of Europe 2014 https://rm.coe.int/16800cce5b 34-35 #204.
86 Council of Europe 2014 https://rm.coe.int/16800cce5b 35 #209.
87 Council of Europe 2014 https://rm.coe.int/16800cce5b 38-39 #223-224.
88 Council of Europe 2014 https://rm.coe.int/16800cce5b 39-40 #228.
89 Council of Europe 2014 https://rm.coe.int/16800cce5b 40 #232-233.

witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings", parties will consult on either one venue for prosecution or which country will prosecute which accused.[90]

36. The Report comments that "[p]aragraph 2 [of Article 27] requires the establishment of a central authority or authorities responsible for sending and answering requests for assistance".[91] This is a useful provision for consideration in the context of South African legislation. I would, however, add the proviso of an independent body.

37. Paragraph 8 allows for a Party to include in its request a further appeal that "the fact and content of the request be kept confidential". This is an equally useful provision which could be applied in the South African context since organisations are often reluctant to comply with the requirement of the mandatory reporting of cyberattacks as this may lead to reputational damage. The fine proposed (R 50 000) for failure to report[92] is ineffective, if not meaningless, since companies would in general rather pay this sanction than suffer the reputational pushback by reporting successful cyberattacks on their systems. Similarly, "If the requested Party cannot comply with the request for confidentiality, it shall notify the requesting Party, which then has the option of withdrawing or modifying the request."[93] This is a good idea for (re)consideration in the context of the *Cybercrimes Act*.

38. Since computer data are highly volatile, meaning they could be altered or deleted or (re)moved at will, thereby destroying evidence of the identity of the perpetrator or evidence of guilt, Article 16 provides for the introduction of legislation at the domestic level which would allow for "the expeditious preservation of data stored in the territory of the requested Party".[94]

In addition to these useful and thought-provoking provisions in the *Budapest Convention,* South Africa also stands to learn lessons from other African countries.

90 Council of Europe 2014 https://rm.coe.int/16800cce5b 41 #239.
91 Council of Europe 2014 https://rm.coe.int/16800cce5b 47 #265-266.
92 Section 54(3) of the *Cybercrimes Act*.
93 Council of Europe 2014 https://rm.coe.int/16800cce5b 49 #273.
94 Council of Europe 2014 https://rm.coe.int/16800cce5b 50 #282.

## 3 The African Union's *Convention on Cyber Security and Personal Data Protection* as well as the East African experience

Many African countries have adopted and benefitted from the African Union's *Convention on Cyber Security and Personal Data Protection*.[95] For example, Rwanda National Computer Security and Response Centre (inaugurated in 2015) detects, prevents and responds to cyber security threats (quoted in Muendo [2019] - the source is unavailable to me). Its National Cyber Contingency Plan, on the other hand, handles cyber crises (also quoted in Muendo [2019] - the original source is unavailable to me). In addition, cyber security awareness is taken very seriously in Rwanda. A cyberattack on Equity Bank, which relies heavily on digital, cross-border banking services,[96] was prevented in November 2019 acting on a tip-off from a member of the public after the syndicate successfully hit branches of the same bank in Kenya and Uganda.[97]

Similarly Kenya launched its National Cyber Security Strategy in 2014 to raise cyber security awareness and equip the country to face cyber threats. Generally, remarks Mercy Muendo, "Kenya has a robust cyber security policy which includes a legal and regulatory framework. The result has been that impending cyber attacks [sic] are discovered before massive damage is done and ongoing attacks are rapidly arrested."[98]

Uganda for its part has a national computer emergency response team[99] in place in addition to a National Information and Technology Authority[100] that provides cyber security training as well as technical support on a national level. These measures, among others, have boosted the country's cyber security strategy and safety. Muendo[101] suggests in a thoughtful piece that while Africa's digital infrastructure is on the whole poorly equipped to face the continent's intensifying cyber-security threats and risks,[102] Kenya and Rwanda, for their parts, "are two of the top three cyber secure countries in Africa".[103] On the face of it these observations reflect poorly on South Africa,

95 African Union *Convention on Cyber Security and Personal Data Protection* (2014).
96 Muendo 2019 https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.
97 Wambui 2019 https://nation.africa/kenya/news/Rwanda-busts-bank-hackers-ring-targeting-Equity-Bank/1056-5332858-ehye3p/index.html.
98 Muendo 2019 https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.
99 Uganda Communications Commission 2023 https://ug-cert.ug/.
100 NITA Uganda 2023 https://www.nita.go.ug/.
101 Muendo 2019 https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.
102 Serianu 2017 https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf.
103 ITU 2018 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

which is not only the second largest economy on the continent (after Nigeria) but also the most developed country in Africa.

Against the backdrop of this very fruitful discussion on what we stand to learn from the *Budapest Convention* and the African Union's *Convention on Cyber Security and Personal Data Protection,* I shift the focus to another jurisdiction, namely Australia, to assess what could be learned from its cybersecurity culture to possibly enrich South Africa's approach as embodied in the *Cybercrimes Act* and related legislation. In other words, how does South Africa's cyber security culture measure up against the exemplary legal and policy framework outlined below?[104] I accordingly proceed to consider the matter from a South African perspective vis-à-vis Australia.

## 4 What's happening in Australia?

Just as South Africa's unique energy needs produced a government minister for electricity, Clare O' Neil became Australia's Minister for Cyber Security (although her portfolio was combined with that of Home Affairs). In what follows I consider her outstanding contribution to Australia's cybersecurity culture, and in doing so I am particularly interested in what South Africa can learn from this strategy.

Three of the most innovative reforms which she highlights[105] are the formation of a proactive new (federal) task force (comprising 100 of the top cyber experts in Australia) by the federal government (to essentially "hack[ing] the hackers"), making payment of a ransom demand illegal and ensuring that the retention of sensitive personal data be curtailed as much as possible (to prevent its exposure after a hack). For example, in the case of the Medibank hack, Medibank being the Australian health insurer, that affected almost 10 million customers, the Australian Federal Police (AFP) managed to disrupt the Russian group responsible (possibly "REvil", which is protected by Putin himself and operates as a business entity. When their demands were not met those responsible proceeded to publish this highly sensitive hacked data on the Dark Web.[106] Together with the Optus incident, these two cyber breaches present "two of the most significant data breaches in Australia's history".[107]

---

104 Muendo 2019 https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.

105 Lapham 2022 https://www.abc.net.au/news/2022-11-13/medibank-data-breach-cybersecurity-latest/101648178.

106 Judd and Walker 2022 https://www.abc.net.au/news/2022-11-11/afp-reveal-more-information-on-medibank-hacker/101643794.

107 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf 14.

O'Neil emphasised that the best outcome should not be the imprisonment of cyber criminals but rather a robust strategy for proactively disrupting their operations. These groups or hacking farms or individuals are often shielded by unfriendly foreign governments. In this respect it is worth noting that AFP Commissioner Reece Kershaw confirmed that "the AFP was scouring the internet and dark web for those accessing the information and attempting to profit from it [the data illegally stolen by way of the Medibank hack]".[108] My view is that the threat of punishment has its limitations and that there is an urgent need for innovative strategies to *proactively combat* cyber threats (my emphasis).

Finally, on 8 December 2022 Clare O' Neil announced a blueprint for the development of the country's 2023-2030 Australian Cyber Security Strategy.[109] Public submissions to the discussion paper were invited and the window ran from 27 February 2023 to 15 April 2023.[110] Once again this highlights the valuable contribution of the public in improving national cyber security culture.

In terms of the strategy, the national government has an obligation to envision a secure cyber space for a resilient online business community as its vision for 2030.[111] To build collaborative cyber resilience as part of its national security, three matters deserve attention. These are: "governments protecting against sophisticated cyber threats, businesses protecting their customers, and the community making cyber-aware choices".[112] Effective cyber security demands that reporting obligations[113] must be taken seriously.[114] The reason for this, of course, is to ensure that the cyber security task force is aware of new developments in the form of novel or innovative cyber breaches or attacks and the sharing of the "root cause findings from investigations of major cyber incidents so that we can all

108 Judd and Walker 2022 https://www.abc.net.au/news/2022-11-11/afp-reveal-more-information-on-medibank-hacker/101643794.

109 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf.

110 Australian Government 2023a https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/alternative-commonwealth-capabilities-for-crisis-response-discussion-paper.

111 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf 11.

112 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf 12.

113 Section 54(1) of the *Cybercrimes Act*.

114 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf 17.

benefit from these learnings".[115] But there are very real problems or challenges with this notion in the South African milieu. A very relevant idea is the suggestion that the government's departments and agencies should serve as a model for best practices in respect of a safe cyber security culture and responsible risk management planning.[116] How feasible the application of this magnificent initiative would be in the current South African context is of course an open question. In building a resilient and secure cyber secure ecosystem, remediation (effective post-incident review) and exploring opportunities to enhance support to victims of cybercrime are essential cornerstones.[117] Finally, emerging technologies such as quantum communication technologies, the Internet of Things and artificial intelligence have already impacted on or are bound to impact on and disrupt the cyber security landscape shortly and it is vital to keep track of these developments.[118]

Against the background of the international cyber security culture, as evidenced by generally accepted best practices embodied in the legislative framework and/or practice in Australia, I accordingly proceed to critique the South African *Cybercrimes Act* as follows.

## 5 A comparative/constructive critique of the *Cybercrimes Act* 19 of 2020

Although the Act commenced on 1 December 2021 by Presidential decree, certain sections of the Act are not yet operational.

In concluding his overview of the *Cybercrimes Act*, Mtuze remarks that:

> [t]he Cybercrimes Act, in regulating the entire terrain of cybercrime as it is perceived currently, offers greater legal protection for victims of cybercrimes, guidance to law enforcement agencies and legal certainty for the courts. The creation of specific offences as well as sentences is a move towards more efficient cybercrime regulation than was previously afforded in terms of the common law and ECTA.[119]

That might be so, but as I argue below, there is still considerable room for improvement to make South Africa a robust, cyber-secure space. Even though Sizwe Snail ka Mtuze may not be quite an objective observer and

115 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf 20.

116 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf 19.

117 Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf 21.

118 Perlroth *This is How They Tell Me the World Ends* generally.

119 Snail ka Mtuze 2022 *Obiter* 559-560.

commentator (he was involved in advising for and drafting the Act), it is nonetheless true that the new Act is a considerable improvement on the piece-meal provisions and the less than satisfactory wording of its predecessors, which preceded the promulgation, albeit not the inauguration, of the Act as a whole. I will attempt to demonstrate the need for some of the more pressing concerns to be addressed, along the following lines:

1. The preparedness/effectiveness of SAPS to handle complex cybercrime/investigations should be thoroughly examined. Australia's federal cyber task force (packed with 100 of the country's top cyber experts) option appears to be the best practice and should be adopted. Crucial questions to be considered relate to SAPS's potential deficiency in managing cybercrime reporting, which may potentially impede investigations, given that the *Cybercrimes Act* is heavily dependent on competent enforcement authorities.

2. Is there a special task force in place within SAPS to handle cyber incident reporting? If so, does the task force have the necessary specialised skills and resources to enforce the Act? The answer to these questions is a resounding negative and, considering the wealth embedded in the Australian experience of the value of such a task force, this appears to be a drawback that demands rectification.

3. Will this obscurity compromise criminal procedure and aspects thereof? This is almost a foregone conclusion and requires careful deliberation to ensure smooth prosecutions.

4. Critics have argued that the definition of "cybercrime" within the Act is far too broad and this raises concerns that legitimate activities may fall under this broad definition, leading to legal uncertainties.

5. Does South Africa, like the US and Australia, have a national cybersecurity strategy which the Act can be integrated into, to ensure effective and robust cyber resilience – in both the public and the private sector? Obama was clear when he mentioned that national and economic security depends on the sound reliability of a nation's critical infrastructure.[120]

6. One of the most cogent points of criticism is failure to engage in enhancing international cooperation. Does the Act contain a framework for international cooperation? I argue that it does not. It does reference provisions for extradition and mutual legal assistance but seems to lack specificity. In the absence of an effective mechanism

120 CISA 2013 https://www.cisa.gov/resources-tools/resources/executive-order-eo-13636-improving-critical-infrastructure-cybersecurity.

to foster international cooperation, this represents a serious lack. How effective is the Act in this regard? Clare O'Neil has mandated the outlawing of ransom payment for data recovery from hacking, but South Africa's legislation contains no such provisions. This will require buy-in from the private sector, advocacy groups, policymakers and the public at large.

7. The Act notably neglects crucial aspects of cybersecurity awareness and training, which is pivotal when it comes to protecting the integrity of our organisations and national security. Both the East African and the Australian experiences have demonstrated how valuable cybersecurity awareness is. It is worth noting that effective cybercrime prevention hinges on educating both the public and the private sectors.

8. It is also important for the Act to make a paradigm shift from punitive to proactive prevention and disruption, as the Australian experience has so pointedly shown. Following instead the *Budapest Convention*'s emphasis on punitivity as the Act does is a mistake.

9. The issue of an obligation to report cyber breaches to the SAPS remains a sensitive point. I suggest an independent agency which would agree to confidentiality unless the identity of the victim is essential for the case to be used for heuristic purposes. In *Black Sash Trust v Minister of Social Development* the court ruled:[121]

> SASSA is under a duty to ensure that the payment method it determines … contains adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister … precludes a contracting party from inviting beneficiaries to "opt-in" to the sharing of confidential information for the marketing of goods and services.

By analogy, a confidentiality clause would encourage victims to report, but the point of reporting, as the Australian experience shows, is precisely to learn from cyberattacks. It does not seem as though the rationale for reporting has made an impact on the South African cyber environment, which renders the requirement moot. In the perceptive words of Singh,[122] "[b]oth listed companies and state-owned enterprises face an evergrowing [sic] risk from cyber-attacks [sic] because of their increasing reliance on digital transactions". This is, of course, as true of South Africa as of anywhere else in the world but, as I argue in the introduction to this paper, South Africa is particularly at risk of cyberwarfare. Furthermore, it is important to note that a successful attack could have one or more of the

---

121 *Black Sash Trust v Minister of Social Development* 2017 3 SA 335 (CC) 337 para 10.

122 Singh 2021 https://theconversation.com/south-african-enterprises-cant-ignore-the-risk-of-cyber-attacks-the-threat-is-on-the-rise-166133.

following consequences for the affected company or state-owned enterprise:

1) the jeopardising of a company's access to essential processes integral to operations and the loss of sensitive data;

2) the loss of intellectual property and trade secrets through theft;

3) reputational damage; and

4) significant financial losses.[123]

Finally, to its credit, the legislature proceeded to insert section 18 of the Act,[124] which provides that where the evidence does not prove the commission of a particular offence but instead of another, the principle of substance over form in criminal proceedings shall prevail, which is a principle well entrenched in our law.[125]

## 6 Conclusion

Cybercrime is an urgent global challenge, and the Act does not adequately address the crucial issue of international cooperation. As my overview of the Act and of the related legislative instruments has shown, the South African legislative framework to prevent cyberattacks is somewhat inadequate and requires significant enhancement for South Africa to be a serious global player in the fight against cybercrime. Measures have been suggested and motivated to substantially improve this state of affairs. Collaborative efforts are essential to combat cyber threats effectively, and South Africa must work more closely with international partners. The goal is to enable jurisdictions to join hands in rejecting ransom demands outright and in encouraging companies and government departments to delete non-essential data and proactively disrupting hackers' activities, as Clare O'Neil and the Australian Specialised Federal Cyber Task Force have set out to do. Furthermore, both the East African and Australian experiences have demonstrated the great benefit of involving the public in general in cyber security and crime awareness. I argue that this illustrates the point that legislative measures alone are insufficient to secure robust cybersecurity spaces.

123 Singh 2021 https://theconversation.com/south-african-enterprises-cant-ignore-the-risk-of-cyber-attacks-the-threat-is-on-the-rise-166133.

124 Section 18 of the ECTA.

125 In *Van der Walt v S* 2020 11 BCLR 1337 (CC) para 23 the court held that "an accused is not at liberty to demand the most favourable possible treatment under the guise of the fair trial right. A court's assessment of fairness requires a substance over form approach. The State correctly submits that the question is accordingly whether the Regional Magistrate committed irregularities or deviated from the rules of procedure aimed at a fair trial, and if so, whether they were of the kind to render the trial unfair".

I suggest that exploring and learning from the Australian model is immensely valuable and may address shortcomings or deficiencies in the *Budapest Convention*, on which the *Cybercrimes Act* was largely based, such as an oversized confidence and overreliance on punitive measures.

A need to support victims of cyber incidents has also been identified and measures suggested to remedy this situation. To this end, poststructuralism assisted me greatly in its attenuation of nuance and contradiction. Finally, and in a broader context, the comparative analysis highlights the benefits derived from learning from other cyber security ecosystems. It is my hope that this contribution will encourage other researchers and in particular cyber criminologists to explore other profitable angles in a comparative context. The lessons learned, if widely disseminated, can only benefit the collective advancement of cyber security.

## Bibliography

### Literature

Grobler *Crossing the Line*
Grobler L 2013 *Crossing the Line: When Cops Become Criminals* (Jacana Auckland Park 2013)

Hillman *Digital Silk Road*
Hillman JE 2021 *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (Profile Books London 2021)

Lötter and Bradshaw 2022 *Acta Academica*
Lötter C and Bradshaw G "Reconceptualising Afrophobia in Post-Apartheid South Africa: A Conflict Transformational Perspective" 2022 *Acta Academica* 24-50

Perlroth *This is How They Tell Me the World Ends*
Perlroth N *This is How They Tell Me the World Ends: The Cyber Weapons Arms Race* (Bloomsbury New York 2022)

Snail ka Mtuze 2022 *Obiter*
Snail ka Mtuze S "The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013" 2022 *Obiter* 536-569

Van Niekerk 2017 *African Journal of Information and Communication*
Van Niekerk B "An Analysis of Cyber-Incidents in South Africa" 2017 *African Journal of Information and Communication* 113-132

Watney "Cybercrime"
Watney M "Cybercrime and the Investigation of Cybercrime" in Papadopoulos S and Snail ka Mtuze S (eds) *Cyberlaw @ SA: The Law of the Internet in South Africa* 4th ed (Van Schaik Pretoria 2021) 470-490

**Case law**

*Black Sash Trust v Minister of Social Development* 2017 3 SA 335 (CC)

*Fourie v Van der Spuy and De Jongh Inc* 2020 1 SA 560 (GP)

*Jafta v Ezemvelo KZN Wildlife* (D204/07) [2008] ZALC 84 (1 July 2008)

*Narlis v South African Bank of Athens* 1976 2 SA 573 (A)

*Okundu v S* (CA&R117/16) [2016] ZAECGHC 131 (22 November 2016)

*R v Douvenga* (District Court of the Northern Transvaal, Pretoria) (unreported) case number 111/150/2003 of 19 August 2003

*S v Harper* 1981 2 SA 638 (D)

*S v Manuel* 1953 4 SA 523 (A)

*S v Motata* (Johannesburg District Court) (unreported) case number 63/968/07

*S v Van den Berg* 1991 1 SACR 104 (T)

*State v Howard* (Johannesburg Regional Magistrates Court) (unreported) case number 41/258/02

*Van der Walt v S* 2020 11 BCLR 1337 (CC)

**Legislation**

*Constitution of the Republic of South Africa*, 1996

*Cybercrimes Act* 19 of 2020

*Electronic Communications and Transactions Act* 25 of 2002

**International instruments**

African Union *Convention on Cyber Security and Personal Data Protection* (2014)

Council of Europe *Convention on Cybercrime (ETS No 185)* (2001)

Council of Europe *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence* (2021)

## Internet sources

Australian Government 2023a https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/alternative-commonwealth-capabilities-for-crisis-response-discussion-paper
Australian Government 2023a *Alternative Commonwealth Capabilities for Crisis Response Discussion Paper* https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/alternative-commonwealth-capabilities-for-crisis-response-discussion-paper accessed 10 October 2023

Australian Government 2023b https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf
Australian Government 2023b *2023-2030 Australian Cyber Security Strategy - Discussion Paper* https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf accessed 10 October 2023

Baker 2023 https://www.nytimes.com/2023/10/13/us/politics/north-korea-weapons-russia-ukraine.html
Baker P 2023 *North Korea Shipped Arms to Russia for Use in Ukraine, US Says* https://www.nytimes.com/2023/10/13/us/politics/north-korea-weapons-russia-ukraine.html accessed 15 October 2023

CISA 2013 https://www.cisa.gov/resources-tools/resources/executive-order-eo-13636-improving-critical-infrastructure-cybersecurity
Cybersecurity and Infrastructure Security Agency, United States 2013 *Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity* https://www.cisa.gov/resources-tools/resources/executive-order-eo-13636-improving accessed 14 October 2023

Council of Europe 2001 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
Council of Europe 2001 *Details of Treaty No 185* https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 accessed 28 September 2023

Council of Europe 2014 https://rm.coe.int/16800cce5b
Council of Europe 2014 *Explanatory Report – ETS 185 – Cybercrime (Convention)* https://rm.coe.int/16800cce5b accessed 3 October 2023

Council of Europe 2023a https://coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe 2023a *The Budapest Convention (ETS No. 185) and Its Protocols* https://coe.int/en/web/cybercrime/the-budapest-convention accessed 28 September 2023

Council of Europe 2023b https://www.coe.int/en/web/cybercrime/home
Council of Europe 2023b *Why and How is the Council of Europe Working Against Cybercrime?* https://www.coe.int/en/web/cybercrime/home accessed 28 November 2023

Dover 2023 https://theconversation.com/russian-and-north-korea-artillery-deal-paves-the-way-for-dangerous-cyberwar-alliance-213583
Dover RM 2023 *Russian and North Korea Artillery Deal Paves the Way for Dangerous Cyberwar Alliance* https://theconversation.com/russian-and-north-korea-artillery-deal-paves-the-way-for-dangerous-cyberwar-alliance-213583 accessed 28 September 2023

FBI 2023 https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom
Federal Bureau of Investigation 2023 *FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com* https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom accessed 28 September 2023

Global Initiative Against Transnational Organised Crime 2023 https://globalinitiative.net/analysis/ocindex-2023/
Global Initiative Against Transnational Organised Crime 2023 *Global Organized Crime Index* https://globalinitiative.net/analysis/ocindex-2023/ accessed 28 September 2023

Goba 2023 https://www.msn.com/en-za/news/other/sandf-maintains-it-was-not-hacked-claims-it-may-be-an-inside-operation-instead/ar-AA1gazoh
Goba T 2023 *SANDF Maintains It Was Not Hacked, Claims It May Be an Inside Operation Instead* https://www.msn.com/en-za/news/other/sandf-maintains-it-was-not-hacked-claims-it-may-be-an-inside-operation-instead/ar-AA1gazoh accessed 4 September 2023

ITU 2018 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
International Telecommunication Union 2018 *Global Cybersecurity Index* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf accessed 5 October 2023

Judd and Walker 2022 https://www.abc.net.au/news/2022-11-11/afp-reveal-more-information-on-medibank-hacker/101643794
Judd B and Walker L 2022 *Russia Responds After AFP Commissioner Says Medibank Hackers Based in Russia* https://www.abc.net.au/news/2022-11-11/afp-reveal-more-information-on-medibank-hacker/101643794 accessed 10 October 2023

Lapham 2022 https://www.abc.net.au/news/2022-11-13/medibank-data-breach-cybersecurity-latest/101648178
Lapham J 2022 *Cyber Security Minister Clare O'Neil Flags Multiple Reforms to Protect Personal Data After Medibank Data Leaks* https://www.abc.net.au/news/2022-11-13/medibank-data-breach-cybersecurity-latest/101648178 accessed 10 October 2023

Lötter 2023a https://mg.co.za/thoughtleader/2023-06-08-sleeping-with-the-enemy-the-rise-of-the-insider-threat-in-cybercrime/
Lötter C 2023a *Sleeping with the Enemy: The Rise of the Insider Threat in Cybercrime* https://mg.co.za/thoughtleader/2023-06-08-sleeping-with-the-enemy-the-rise-of-the-insider-threat-in-cybercrime/ accessed 26 September 2023

Lötter 2023b https://mg.co.za/thoughtleader/2023-09-04-cybercrime-the-silent-spectre-of-insider-threats/
Lötter C 2023b *Cybercrime: The Silent Spectre of Insider Threats* https://mg.co.za/thoughtleader/2023-09-04-cybercrime-the-silent-spectre-of-insider-threats/ accessed 26 September 2023

Muendo 2019 https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240
Muendo M 2019 *What's Been Done to Fight Cybercrime in East Africa* https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240 accessed 29 September 2023

NCSI 2023 https://resources.cdn.seon.io/uploads/2023/04/Cybersecurity_countries-min.pdf
National Cyber Security Index 2023 *National Cyber Security Index (NCSI)* https://resources.cdn.seon.io/uploads/2023/04/Cybersecurity_countries-min.pdf accessed 27 September 2023

NITA Uganda 2023 https://www.nita.go.ug/
National Information and Technology Authority Uganda 2023 *National Information and Technology Authority* https://www.nita.go.ug/ accessed 5 October 2023

Olivier 2013 http://thoughtleader.co.za/bertolivier/2013/05/24/modernismpostmodernism-and-poststructuralism-the-difference/
Olivier B 2013 *Modernism, Postmodernism and Poststructuralism: The Difference* http://thoughtleader.co.za/bertolivier/2013/05/24/modernismpostmodernism-and-poststructuralism-the-difference/ accessed 15 July 2024

Sabbagh 2023 https://www.theguardian.com/technology/2023/apr/19/russian-hackers-want-to-disrupt-or-destroy-uk-infrastructure-minister-warns
Sabbagh D 2023 *Russian Hackers Want to "Disrupt or Destroy" UK Infrastructure, Minister Warns* https://www.theguardian.com/technology/|2023/apr/19/russian-hackers-want-to-disrupt-or-destroy-uk-infrastructure-minister-warns accessed 28 September 2023

Sayer 2021 https://theconversation.com/nigerian-museums-must-tell-stories-of-slavery-with-more-complexity-and-nuance-169785
Sayer F 2021 *Nigerian Museums Must Tell Stories of Slavery with More Complexity and Nuance* https://theconversation.com/nigerian-museums-must-tell-stories-of-slavery-with-more-complexity-and-nuance-169785 accessed 16 May 2024

Serianu 2017 https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf
Serianu 2017 *Africa Cyber Security Report: Demystifying Africa's Cyber Security Poverty Line* https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf accessed 5 October 2023

Singh 2021 https://theconversation.com/south-african-enterprises-cant-ignore-the-risk-of-cyber-attacks-the-threat-is-on-the-rise-166133
Singh H 2021 *South African Enterprises Can't Ignore the Risk of Cyberattacks: The Threat is on the Rise* https://theconversation.com/south-african-enterprises-cant-ignore-the-risk-of-cyber-attacks-the-threat-is-on-the-rise-166133 accessed 26 September 2023

Uganda Communications Commission 2023 https://ug-cert.ug/
Uganda Communications Commission 2023 *Computer Emergency Response Team* https://ug-cert.ug/ accessed 5 October 2023

Wambui 2019 https://nation.africa/kenya/news/Rwanda-busts-bank-hackers-ring-targeting-Equity-Bank/1056-5332858-ehye3p/index.html
Wambui M 2019 *Kenyans Arrested in Rwanda Bank Hackers Ring Bust* https://nation.africa/kenya/news/Rwanda-busts-bank-hackers-ring-targeting-Equity-Bank/1056-5332858-ehye3p/index.html accessed 5 October 2023

## List of Abbreviations

| | |
|---|---|
| AFP | Australian Federal Police |
| CISA | Cybersecurity and Infrastructure Security Agency |
| ECTA | Electronic Communications and Transactions Act 25 of 2002 |
| FBI | Federal Bureau of Investigation |
| FSB | Federal Security Service of the Russian Federation |
| ITU | International Telecommunication Union |
| NCSI | National Cyber Security Index |
| NITA | National Information and Technology Authority |
| RSA | Republic of South Africa |
| SANDF | South African National Defence Force |
| SAPS | South African Police Service |
| UK | United Kingdom |
| US | United States |