The Influence of South Africa's Democratic Principles on its Cybersecurity Framework and Cyber Threat Response: A Qualitative Inquiry

Venencia Paidamoyo Nyambuya
Nirmala Devi Gopal
Criminology
University of KwaZulu-Natal
paidanyasha11@gmail.com

Abstract

This study explores the intricate relationship between South Africa's democratic political system, its commitment to human and private rights, and the development of its cybersecurity framework, strategy, and response to cyber threats. Given the country's robust constitutional commitment to human rights, this research explores how these democratic principles are integrated into and influence cybersecurity policies and practices. Through a comprehensive analysis of legislative documents, policy frameworks, this study identifies the extent to which democratic values and human rights considerations shape South Africa's approach to cybersecurity.

The findings reveal that South Africa's cybersecurity strategy is deeply influenced by its democratic ethos, with a strong emphasis on protecting individual rights while ensuring national security. The study highlights how laws such as the Protection of Personal Information Act (POPIA) and the Cybercrimes Act balance the need for security with the protection of privacy and freedom of expression. Furthermore, it explores the multi-stakeholder approach adopted by South Africa, emphasizing public participation, transparency, and accountability in developing and implementing cybersecurity measures. This research also explores the challenges and tensions that arise from striving to protect human rights within the cybersecurity domain, such as ensuring privacy and freedom of information in the face of increasing cyber threats. The study provides insights into how South Africa navigates these challenges, including the mechanisms put in place to ensure oversight and accountability in the surveillance and data collection practices by state security agencies.

Keywords: cybersecurity framework, cyber threat response, democratic principles, influence, South Africa

An overview of the Cybersecurity landscape in South Africa

A cybersecurity framework refers to a structured approach to securing digital environments, protecting sensitive data, and mitigating cyber threats. It aligns with democratic principles by ensuring the privacy of individuals, promoting transparency in data governance, and safeguarding digital rights critical to freedom and equality (Nasir et al., 2024). South African democratic principles include transparency, accountability, equality, the protection of human rights, and the promotion of social justice (Thipanyane, 2015). Important to note is that South Africa's cyberlaws are coordinated by different government agencies, creating windows of opportunities for inconsistencies, fragmentation, and misalignment, thus, weakening initiatives for an effective national cybersecurity strategy (Chigada, 2023). Mahlobo (2015) also acknowledges that different government agencies have overlapping mandates resulting in information asymmetries and poor coordination. Pokwana and Kyobe (2016) posit that civil society, public and private sector institutions are not well-versed with cybercrimes, let alone understanding and interpretation of legislation. Thus, firms and individuals fail to comply with cyber legislation. With reference to the prevailing circumstances, this study also analyses the gaps in the country's cyberlaws and ascertain if the substantive laws criminalise and successfully prosecute cybercrimes. Furthermore, the researcher states that to successfully investigate and prosecute cybercriminals, the legal fraternity, cyberlaws and well-equipped and trained well-trained law enforcement agencies should be pooled together and work harmoniously.

Methodology

For the purposes of data collection researchers made use of academic journals, government reports, policy documents, official statements, and other relevant literature to gather data. The researchers conducted a thorough literature review to identify existing studies, reports, articles, and other publications relevant to South Africa's political system, human rights protections, cybersecurity framework, strategy, and cyber threat response. This review helped them understand the current state of knowledge in the field and identify gaps or areas requiring further investigation.

Once the data were collected, the researchers screened and selected relevant sources based on predetermined inclusion and exclusion criteria. Researchers focused on sources that provided in-depth insights into the influence of South Africa's democratic political system and human rights protections on its cybersecurity landscape. We prioritised recent and authoritative sources to ensure the relevance and accuracy of the information.

After compiling a comprehensive dataset, the researchers analysed the gathered information using thematic analysis as illustrated by Braun and Clarke (2006) to identify patterns, trends, relevant to our research questions. This analysis accrued several themes as presented in the findings section.

Finally, the researchers interpreted the findings of their data analysis and synthesised the results to draw conclusions about the influence of South Africa's democratic political system and human rights protections on the development of its cybersecurity framework, strategy, and cyber threat response. The implications of our findings and any limitations of the study were discussed, as well as offered recommendations for policymakers or future research directions.

Development of Cyberspace and Cybersecurity in South Africa

By the nature of its political system, South Africa is a democratic state. There is no uniform definition of democracy among scholars, however, it is a political system where the people have the right to govern themselves, civil society can hold their elected representative accountable for actions or inactions, governmental authority is limited by civil rights, and freedoms and equality of all are guaranteed (Sodaro, 2004: 31 & Attenberger, 2020: 14).

Since the end of apartheid and beginning of democratic dispensation in 1994, the African National Congress (ANC) has been in government in South Africa. However, it has been losing its attractiveness to the electorate for reasons not unconnected with internal rifts, and its failures on service delivery (Sutherland, 2017: 84). On one hand, there is an independent and powerful Constitutional Court that holds everyone accountable (Roux, 2016). On the other hand, there is the Parliament that has often struggled to scrutinise complex legislation, and exercises only limited oversight of budgets, ministers and policies (Hawker, 2003; 2007). The later fits broadly within the framework of weak institutional endowments (North, 1990), explaining the limits to the ability of governments to create mechanisms and structures to deal with complex issues. Sutherland (2017) adds that if government is to persuade firms and individuals to adopt measures to improve their cybersecurity, then it needs to ensure its own activities are highly secure or, initially, not embarrassingly insecure, and to acknowledge the limitations of its influence, in order to maximise its credibility. He notes that after 1994, the governance of the intelligence community and of the wider security sector was never going to be easy, given the histories of the State and of the ANC, neither of which had shown much regard for accountability or transparency in intelligence and security matters.

Important to note is that South Africa has had a "shortage of ICT skills for many years despite high levels of unemployment and the presence of many colleges and universities" (Sutherland, 2017: 96). One cause is the lack of a national ICT planning process that could engage with industry, educational institutions, and providers of continuing professional development (CPD). For instance, 86% of South Africans regularly use online banking services (Kshetri, 2019), a proportion higher than many countries in the Middle East and Turkey.

Cyber threats and cybercrimes in South Africa

Cyber threats and actual crimes are global concerns of the contemporary period. Though such security apprehensions are common to all regions, the exact nature of the threat types and motivations vary from one region to the other (Brown & Rudis, 2017). By cybercrime, we mean those offences highlighted by the 2017 Cybercrimes and Cybersecurity Bill. They are: unlawful securing of access; unlawful acquiring of data; unlawful acts in respect of software or hardware tool; unlawful interference of data or computer programme; unlawful acquisition, possession, provision, receipt or use of password access codes or similar data and devices; cyber fraud; cyber forgery and uttering; cyber extortion; theft of incorporeal.

Depending on the impact, perpetrators, target and gravity on victims, cyber-incidents get unequal attention in the public space. For instance, cases of nation-state cyber-espionage, which are closely linked to advanced persistent threats (APTs), will receive significant attention (Van Niekerk, 2017: 114) compared to attacks on private organisations that will as well come under scrutiny for having insecure sites, and toxic to customers. Ransomware is another attack that elicits as much as national and global interest. Notably, the number of ransomware payloads proportionally increased internationally from 18% of detections in January 2016 to 66% in November 2016 (Van Niekerk, 2017: 114). There were 3,700 ransomware attack victims who collectively lost $49.2 million and 800,000 malware attacks where victims collectively lost $45.6 million. Compared with phishing, that is more than 70 times fewer victims (Mabuza, 2022).

Similarly, phishing is another very common threat. According to Surfshark's study, phishing has continued to be the most common cybercrime for the third year (2019-2021) in a row (Mabuza, 2022). In 2020, there were 241,343 phishing victims, while 2021 recorded 323,972. Other security concerns and at the level of a national emergency are: insider threats, either malicious or accidental, resulting in security incidents; attacks by hacktivists who are politically or ideologically motivated; and attacks by individual hackers who are trying to learn or show off, such as the "script kiddies" who make use of existing tools (Andress & Winterfield, 2014).

South Africa has had its fair share of cyber-incidents with heavy toll on the economy too. The country has the familiar odd record of being one of the most often attacked countries in Africa. This is partly due to its demography, continental economic strength, and attendant bourgeoning exposure to the cyberspace. Analysts have projected that 10–15% internet penetration as the threshold level the generation of significant hacking activities (Kshetri, 2013). As of January 2022, there were 41.19 million active internet users in South Africa (Galal, 2023). According to the Statista.com, it was also found that 28 million internet users in the country used social media, which was around 46 per cent of the total population.

In the last decade, South Africans experienced several extensive scamming attacks, of which the most prominent is the herding of personal information using South Africa Revenue Service (SARS), and the fraudulent World Cup offers supposedly from South African Airlines (Grobler & Vuuren, 2013). Their findings revealed that many people have already succumbed to these fraudulent emails that gather their personal information. South African banks are also experiencing an increase in banking fraud that directly poses a threat to individuals that may lose their savings. A 2013 report by Norton found that South Africa had the third highest number of cyber-attacks in the world. It was found that majority of these attacks were conducted by non-South African hackers, who wished to gain access to faster internet and more advanced software. Cybersecurity is an issue for both the public and private sectors (Griffiths, 2017).

The estimated costs of cyber-attacks are as diverse as the nature of the crimes. Estimates in 2011 put the financial loss from cyber-attacks at ZAR 3.7 billion in direct losses and ZAR6.5 billion in indirect costs (Norton South Africa, 2012). In 2014, South Africa was estimated to have lost between ZAR5.8 billion (Sutherland, 2017: 84) and ZAR50 billion to cyber-incidents (Van Niekerk, 2017: 115). Over half a billion online personal records were lost or accessed illegally in South Africa during 2015 (*SABC News*, 2017). The South African Banking Risk Information Centre (SABRIC) estimated that South Africa loses $157 million annually to cyberattacks (Kshetri, 2019). The threat will become more widespread going forward as the number of South African Internet users increase, aided by the African continent's increasing undersea capacity (Song, 2017).

In 2015, one in 10 businesses reported a cyberattack in South Africa (Jonker, 2015). Such incidences were expected to rise significantly from 2018, when reporting was made mandatory, triggering much greater attention to prevention and security, especially because firms can then be held legally liable (Ibid). As at 2022, Surfshark, a cybersecurity company in its research ranked South Africa among the top 10 countries found to have experienced the most cybercrime in 2021 (Mabuza, 2022). South Africa had 52 victims per 1-million internet users, to earn a sixth place in the global ranking that also has countries like United Kindgom, United States, Canada, Austria and Greece in the top five. The Chief Executive Officer of Surfshark, Vytautas Kaziukonis, said as more of our lives become digital, the chances of falling victim to online crimes grow every year. Since 2001, the online crime victim count increased 17 times, and financial losses grew more than 400 times, from $2,000 to $788,000 losses per hour (Mabuza, 2022). In total, cybercrime claimed at least 6,502,323 victims and $26,116bn in losses over the 21-year period (Ibid).

Indeed, there is uncertainty and crisis of confidence in the capability of the South African Police Service (SAPS) to efficiently handle matters of technology and cybercrimes. There are dangers in the lobbying and salesmanship from those making cybersecurity systems, who may overstate the risks and the effectiveness of their products, in order to increase their profits. Equally, the intelligence services may seek greater budgets to buy such systems, an extension of the military-industrial complex described by Eisenhower (Brito & Watkins, 2011).

More specifically, a 2017 analysis of cyber-incidents (through the media lenses) in South Africa critically examined the state of affairs via some 54 incidents that were considered (Van Niekerk, 2017). The study categorised those identified cases according to: (i) impact type, (ii) perpetrator type, and (iii) victim type. The study found that the most common impact type is data exposure and the most prevalent perpetrator type is hacktivists, which had also exhibited a recent increase in activity (ibid: 113). The study established the trend of high number of incidents of data exposure caused by error, a trend running contrary to the drive to improve cybersecurity in South Africa. "It was also found that of the incidents considered, 54 per cent targeted state-owned or political entities as victims (Van Niekerk, 2017: 113-4). The main findings across the theme areas of impact type, penetration type and victim type are illustrated thus.

(i) Impact type

The 54 incidents were examined across six types of impacts of cyber-attacks. They are: exposure of data or records; disruption or denial of service through encroachment; financial motive that succeeded or otherwise in stealing money; defacement of webpages; data corruption and modifications, and system penetration through illegal access to network or system only.

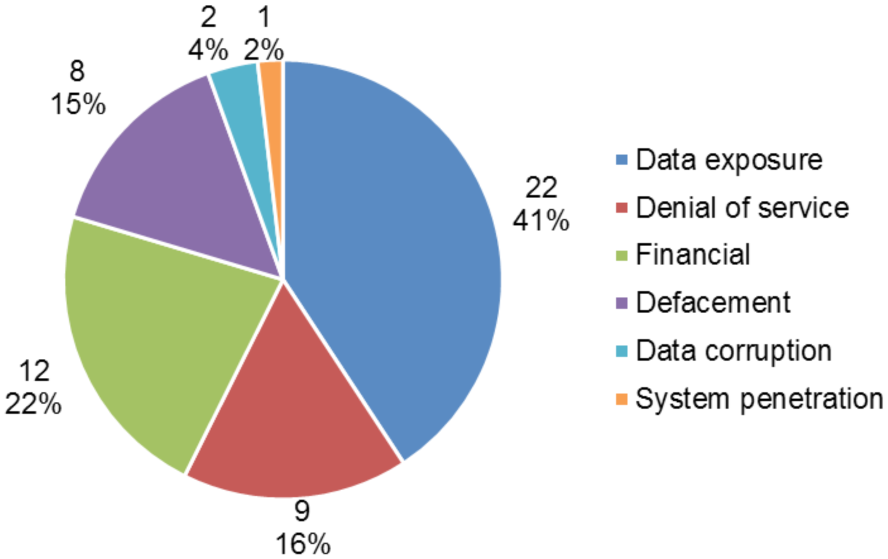


Figure 1: Graphic illustration on impact type findings by the number of sample size. Source: Van Niekerk, 2017:" 117.

Data exposure has been common across private and public organisations, and the study confirmed 22 cases of such attacks coming from within and outside South Africa as at 2017. Van Niekerk captured Advanced Persistent Threat (APTs) infections, where in one of the incidents, an organisation in South Africa fell victim to the APT1 espionage group attributed to Chinese hackers in 2010 (2017: 117). About two years later, "the Red October cyber-espionage campaign (attributed to Russian hackers) was detected, after having possibly operating for five years undetected, with various targets in a number of countries affected, including infecting a diplomatic organisation in South Africa" (Ibid: 118).

In the web of data exposures are targets like the embassies and foreign missions, the hacking of South African Police Service database that released approximately 16,000 details of whistleblowers and victims, hacking of fast-food outlets, accidental data exposure by Vodacom mobile operator, and the invoicing portal of the City of Johannesburg. Not left out is the portal of Cell C mobile operator in 2014, Altech Autopage, the hacking of the South African National Roads Agency Limited (SANRAL) e-Toll website, the job portal of V-Report in 2016, the compromise of state's Government Communication and Information System (GCIS) as part of #OpAfrica's grand data exposure that affected 2500 websites, hacking of the state-owned arms procurement agency Armscor's invoicing portal, Cinema chain like Ster Kinetor, the eThekwini Municipality (Durban) e-services portal, and the e-billing portal of mobile operator MTN, also in 2016 (Ibid). "The Chinese-linked group known as APT10 were involved in the Cloud Hopper espionage campaign in late 2016, or which there were South African victims (Ibid, 119).

Financial motive is just as rife as data exposure, though with lesser proportion as shown above. There are several familiar cases in that respect. In 2003, Absa bank was hacked, and it lost nearly ZAR500, 000 (Thiel, 2004). "Hackers targeted three South African banks in 2006, managing to transfer cash from bank accounts into prepaid accounts held with mobile operators (Van Niekerk, 2017: 119). In July 2009, a criminal gang stole about ZAR7 million from bank accounts that were compromised by phishing and SIM cards duplication for the interception of online banking one-time PIN codes (OTPs). Hackers also compromised Land Bank's IT security in December 2010. The hackers initially stole ZAR8 million that were later recovered by the bank (Potgieter, 2011). It was the turn of PayGate, a credit card payment provider, in August 2012. Hundreds of thousands of credit card details were compromised across four major banks, with an undisclosed loss of fortune (Arde, 2012). The National Department of Water Affairs lost ZAR2.84 million in 2011 when its passwords were compromised. The South African Post Office's financial institution, Postbank, also lost ZAR42 million to hacker in January 2012 (Patrick, 2015). A year later, over ZAR15 million was lost by the Department of Minerals and Energy after login credentials were stolen by criminals using a keystroke logging device (Ibid.). In 2014, insider threats among employees made a botched attempt to hack the payroll system of Eskom – the state-owned electricity company. Almost at that period, the Gautrain Management Agency's bank account nearly lost ZAR800 million to a hack. The Road Traffic Management Corporation was not that lucky in 2015 as it losts ZAR8.5 million to a series of illegal transfer by hackers (Mkhwanazi, 2015).

In denial of services, a case of reference is that of South African petrochemical company's supervisory, control and data acquisition system that was infected by the PE Sality virus in 2009 (Pretorius, 2016). The attack denied operator's visibility of operations for eight hours until the infected servers were recovered. "In 2013, the website of the national ruling party, the African National Congress (ANC), was made inaccessible due to a distributed denial of service (DDoS) attack by Anonymous Africa (different from Anonymous #OpAfrica) (Van Niekerk, 2017: 120). From 2013 to 2015, the *Independent Online* news website, mobile operator MTN and affiliated service providers all suffered a service outage due to DDoS attacks that were targeted and access disrupted. "Anonymous Africa returned in 2016 by targeting the South African Broadcasting Corporation (SABC), whose website was unavailable due to the DDoS attack, with the hackers stating that the attack was in protest against corruption and the recent censoring of protests" (Van Niekerk, 2017: 120). Also targeted in 2016 were the websites of the Economic Freedom Fighters political party, news channel ANN7, *The New Age* newspaper, and computing company, Sahara, "in protest against perceived corruption by their owners and the South African government" (Van Zyl, 2016).

Almost all major institutions – education, health, telecoms, politic and so on – have had encounters with hackers' *defacement* of websites. In 2003, University of Stellenbosch, Natal University, Rhodes University and the University of the Witwatersrand, and University of Cape Town all fell victim of the illegal acts (Van Niekerk, 2017: 120-1). The following year, a total of 45 company websites in Cape Town and Stellenbosch were attacked by Spykids. In January 2005, hackers from Morocco, known as Team Evil, defaced approximately 260 South African websites, replacing the legitimate websites with anti-U.S. messages (Mbongwa & Makua, 2005). In 2008, both the Democratic Alliance political party and the ANC Youth League websites were compromised. While the Democratic Alliance website was offline for a week, the ANC was defaced with a fake message announcing that the youth president has stepped down (Van Niekerk, 2017: 121). From Moroccan hackers came the defacement of three government websites in 2012. The Administrative Adjudication of Road Traffic Offences website was defaced by a Bangladeshi hacker in 2013, who posted a message notifying the website owner to secure the website (*ITWeb*, 2013). Approximately 20 websites, including Sasol, were defaced by a Moroccan hacktivist in 2014, again protesting the South African position on Western Sahara (Ackroyd, 2014).

Notably, the trio of data exposure, denial of service and financial impacts have been the most consistent, with spikes between 2013 and 2016 (Van Niekerk, 2017: 122). As self-evident in Figure 2 below, the financial-crime motivation remained constant, whereas the data exposure and denial of service motivations, often indicators of hacktivism and protest – i.e., they commonly used to discredit or exact revenge – appear to be on the rise in the South African context.

Finally, it is interesting to note that after reaching a total of 11 instances in 2013, there were declines in 2014 (7 instances) and 2015 (2 instances), before a spike to 12 instances in 2016, the largest number recorded for any of the years studied – an apparent indication that cybersecurity measure are still not being effectively applied in South Africa, and/or that attempts at perpetration are becoming increasing complex and skilful (Van Niekerk, 2017: 122).

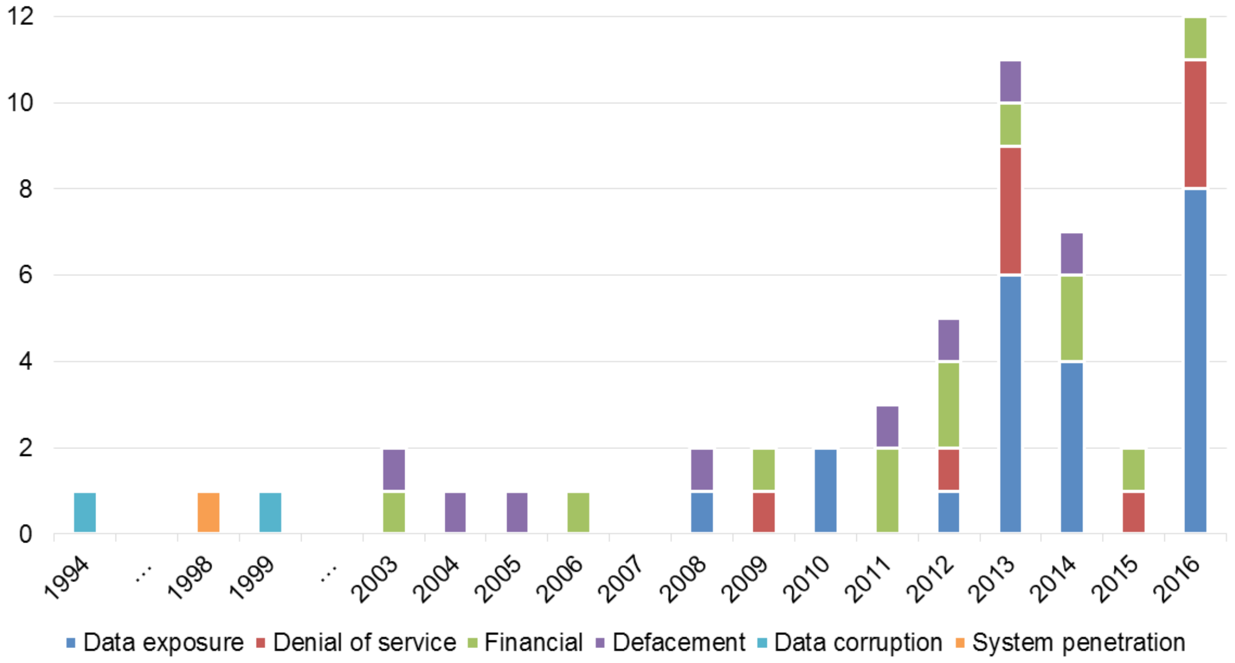


Figure 2: Graphic illustration on trend in impact type. Source: Van Niekerk, 2017.

Perpetrator type

Perpetrators that were uncovered cut across different groups like: hacktivists, individual hacker, insiders, accidental/misconfiguration by non-malicious insiders, malware, and nation-state. Figure 3 below shows the spread of perpetrator types. Threats of hacktivist proved to be the most dominant of the seven types highlighted, and closely followed by threats of criminals, accidental cases, and individual hackers.

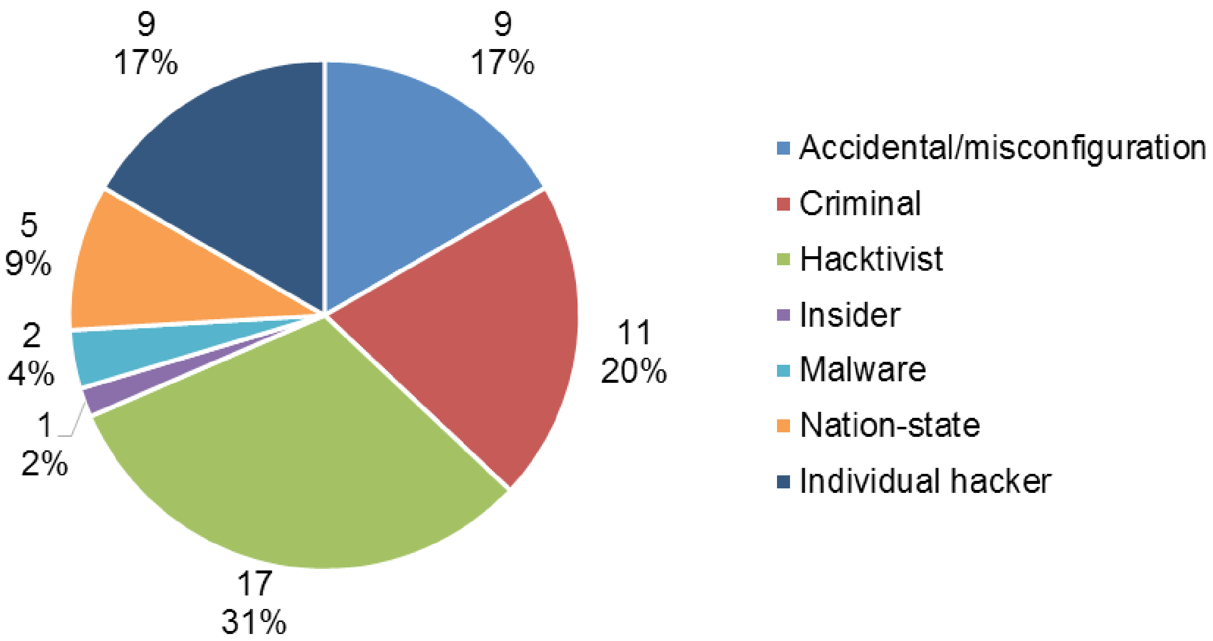


Figure 3: Graphic illustration on perpetrator type. Source: Van Niekerk, 2017: 122.

Figure 4 below shows that the threat of individual hackers has since 1994 always been part of South Africa, though in marginal proportion. Along came the threats of hacktivists, criminal and nation-state. However, these various threats have since 2011 been consolidating to swell the threat levels, "indicating a growing protest and revenge dimension in South Africa's cybersecurity risk profile" (Van Niekerk, 2017: 123).

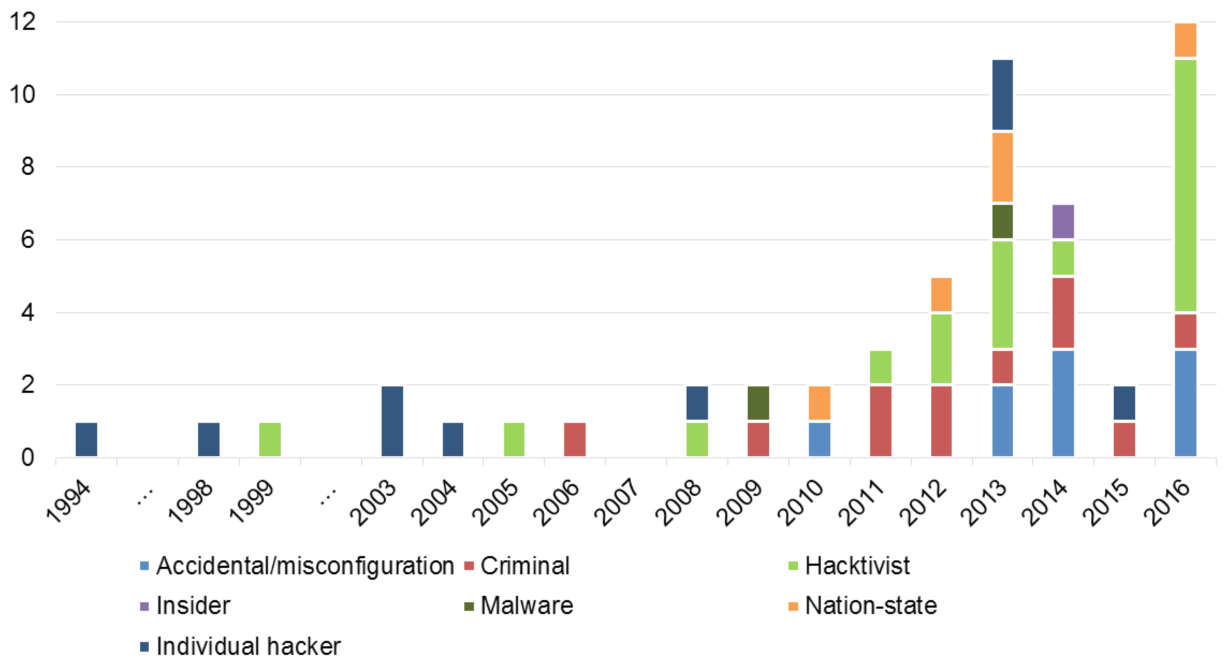


Figure 4: Graphic illustration on perpetrator type trend. Source: Van Niekerk, 2017.

Victim type

In the distribution of the victims, findings by Van Niekerk showed that more than half of the incidents were aimed at State institution and political parties compared to other entities.

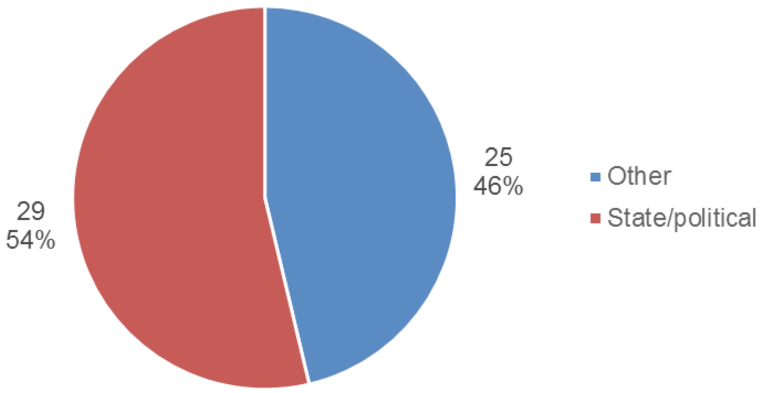


Figure 5: Graphic illustration on victim type. Source: Van Niekerk, 2017.

Figure 6 below expresses the trend in victim type showing that state/political institutions have always been the target of interest in the 1990s, and significantly diminished in the 2000s. The last decade, however, saw a massive spike in cases of cybersecurity threats targeted against state/political institutions and other entities.

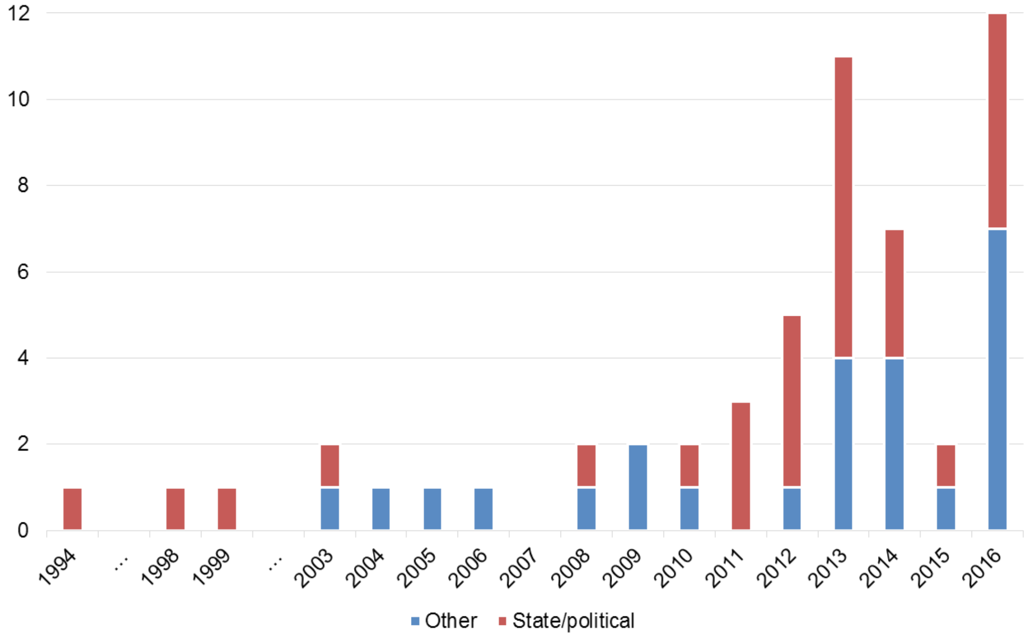


Figure 6: Graphic illustration on victim type trend. Source: Van Niekerk, 2017.

From the foregoing, it is evident that the leading perpetrators of cyber-attacks are hacktivists, and criminals. “The top two cyber-attack impacts are data exposure and financial theft. The top two perpetration-impact combinations are criminals resulting in financial impact, and accidental/misconfiguration resulting in data exposure” (Van Niekerk, 2017: 126). Besides the growing patronage in internet connectivity vis-a-vis cyber threats globally, heightened political tension and negative perceptions on financial mismanagement of the commonwealth in South Africa have spiked attention of protesting hacktivist and criminals alike on State-owned/political party institutions more than on other entities (Ibid).

Cybersecurity policy framework and strategy in South Africa

Certainly, in the face of the cyberspace volatility and threats, the cybersecurity and control mechanism are *prima facia* ineffective. Based on history, South Africa has a common law on right of privacy that dates back to the 1950s, as seen in the O'Keeffe v Argus Printing (1954) case (Sutherland, 2017: 94). However, the foundational acts really took effect from legislation, through the following: (1) Electronic Communications and Transactions Act (ECT) of 2002; (2) The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 2002; (3) The Protection of Personal Information (POPI) Bill (2009); (4) National Cybersecurity Policy Framework (NCPF) 2015, and (5) Cybercrimes and Cybersecurity Bill.

Like other countries, modern South Africa has adopted a variety of approaches to e-government at national, provincial, and municipal levels, purportedly all under the Department of Public Service and Administration, though most recently from DTPS (2017b). Beginning in 1997, there was a slow process of consultation and adoption, aimed at increasing productivity and efficiency for government and improving convenience for citizens. Implementation often failed to achieve the planned goals, due to the limited capacity and the lack of willingness of ministers and officials to engage with the challenges. Little attention was given to cybersecurity, despite risks to human rights from the misuse of the large volumes of personal data held by government, or its theft by cybercriminals.

Suffice to add that the Constitution of 1996 protects privacy in Section 14. It states that everyone has the right to privacy, which includes the right not to have— (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed. Additionally, section 10 created the right to human dignity that must also be respected and protected.

The Constitutional Court has concentrated on forced legislative disclosure of information, providing general guidelines for data protection (SALRC, 2005): Was the information obtained in an intrusive manner? Was the information about intimate aspects of the subject's personal life? Was it provided for one purpose but used for another? Was it disseminated to the press or general public from whom the subject "could reasonably expect such information would be withheld"?

The Electronic Communications and Transactions (ECT) Act of 2002 sets out principles for information protection and created offences of unauthorised access to, interception of and interference with data. However, it appears to have had little practical effect.

The Protection of Personal Information (POPI) Act

The Protection of Personal Information (POPI) Bill (2009) broadly matches the European Union legislation (EU, 1995; 2016), with a view to attracting outsourcing and call centre business, since data cannot be transferred from the EU except to countries with comparable data protection provisions. This reflects efforts over a number of years to attract back office processing and call centre activities to major urban centres (Deloitte, 2015 & Sutherland, 2017).

This South African Act (enforced from 1 July 2020) allows for personal data transferal across borders, provided that the country where this data is to be processed follows regulations/ laws, equivalent to those stated in the POPIA. It was based on the European Data Protection Directive (EU DPD) as well as the Organisation for Economic Co-operation and Development (OCED) principles. This act was also inspired by the data privacy models from the United States of America, the United Kingdom, Canada, and Australia. The POPIA safeguards both juristic and natural persons as data subjects and pertains to both manual and electronic processing of personal information (Baloyi & Kotzé, 2018). This makes international data flow much safer in terms of privacy.

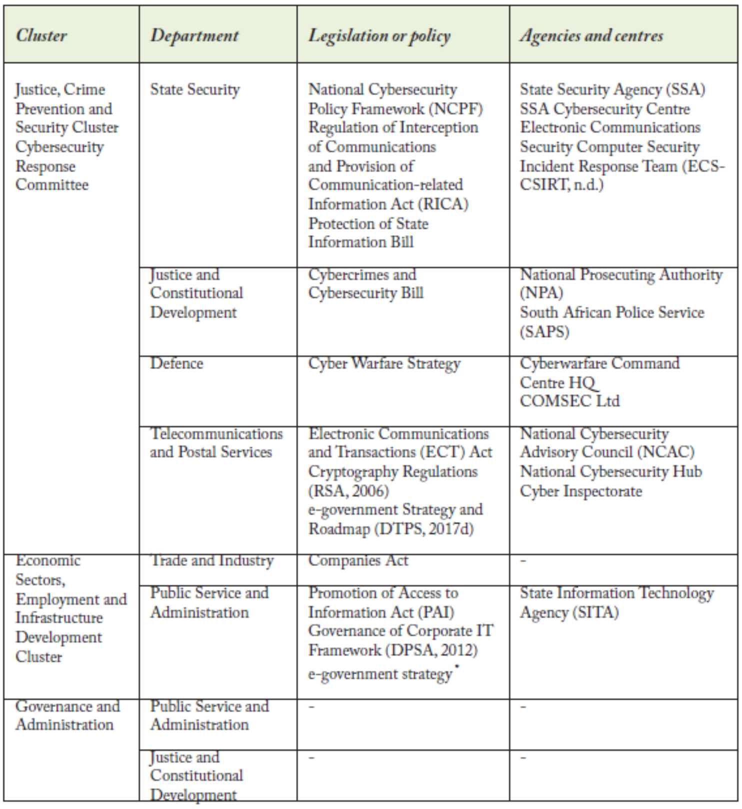
There are eight data privacy principles enlisted in the POPIA, which are derived from the five Fair Information Practices (FIPs). The FIPs are transparency, use limitation, access and correction, data quality and security (Cate, 2006). The eight POPIA principles (section 8 - 25) are accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. If data is to be transferred to a country without such rules and regulations, an agreement can be reached between the parties, with the consent of the individual being mandatory.

According to Sutherland, a central question concerning data protection emerges from section 6(1)(c) of POPI Act. This section excludes processing by or on behalf of a public body involving national security, defence or public safety (2017: 95). This gives the intelligence services an entirely free hand in the processing of data, except that they must comply with Section 198 of the Constitution that, inter alia, enforces human rights. "While those rights can be limited by statute, it is only insofar as is compatible with a democratic society. The subsequent section 6(1)(d) of POPI additionally exempts processing for Cabinet, an obscure provision, since it is in addition to national security purposes, without any indication of what processing the Cabinet might require. Eventually cases must be brought before the Constitutional Court to test the limits of the state to violate the right to privacy" (Sutherland, 2017: 95).

The National Cybersecurity Policy Framework (NCPF)

Acknowledging the lack of coordination within government and the insufficiency of existing legal measures needed to counter and prosecute, the NCPF emerged in 2015 with the aim to: facilitate the establishment of relevant structures in support of cybersecurity; ensure the reduction of cybersecurity threats and vulnerabilities; foster cooperation and coordination between government and private sector; promote and strengthen international cooperation; build capacity and promoting a culture of cybersecurity; and promote compliance with appropriate technical and operational cybersecurity standards (Sutherland, 2017: 91). Implementation of the NCPF requires extensive coordination across government (see Table 1 below), which was unwieldy for effective implementation.

Table 1: Departments directly engaged in cybersecurity



Cluster	*Department*	*Legislation or policy*	*Agencies and centres*
Justice, Crime Prevention and Security Cluster Cybersecurity Response Committee	State Security	National Cybersecurity Policy Framework (NCPF) Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) Protection of State Information Bill	State Security Agency (SSA) SSA Cybersecurity Centre Electronic Communications Security Computer Security Incident Response Team (ECS-CSIRT, n.d.)
	Justice and Constitutional Development	Cybercrimes and Cybersecurity Bill	National Prosecuting Authority (NPA) South African Police Service (SAPS)
	Defence	Cyber Warfare Strategy	Cyberwarfare Command Centre HQ COMSEC Ltd
	Telecommunications and Postal Services	Electronic Communications and Transactions (ECT) Act Cryptography Regulations (RSA, 2006) e-government Strategy and Roadmap (DTPS, 2017d)	National Cybersecurity Advisory Council (NCAC) National Cybersecurity Hub Cyber Inspectorate
Economic Sectors, Employment and Infrastructure Development Cluster	Trade and Industry	Companies Act	-
	Public Service and Administration	Promotion of Access to Information Act (PAI) Governance of Corporate IT Framework (DPSA, 2012) e-government strategy*	State Information Technology Agency (SITA)
Governance and Administration	Public Service and Administration	-	-
	Justice and Constitutional Development	-	-

Source: Sutherland 2017: 88

In 2015, work started on Cybercrimes and Cybersecurity Bill. As at 2017, the draft was still being scrutinised (Sutherland, 2017: 91). The Bill will formally create the Cyber Response Committee to coordinate work across government. The Cybercrimes and Cybersecurity Bill was released in 2015 but has yet to be approved as a law by President Cyril Ramaphosa.

Thus far, South Africa's national security has been shaped by several policies, with four key principles pertaining to national security. These four principles are: (a) National security must reflect the resolve of South Africans as a nation and as individuals, to live in peace and harmony and to be free from fear and want, and to seek a better life; (b) the resolve of South Africans to live in peace and harmony prevents any South African citizens from engaging in armed conflict, nationally and internationally, with exceptions provided in the constitution and national legislature; (c) national security must be pursued in compliance with the national and international law; (d) national security is subject to the authority of the Parliament and the national executive. One of the key inclusions in South Africa's take on national security is human security, which was conceptualised in 1994. The 1996 White paper on Defence further stated that South African national security has been broadened to incorporate not only military and police issues, but also political, economic, social, and environmental matters.

This use of human security, as a means of ensuring national security has been widely criticised due to the broad definition of 'human security' and has been accused to being a means to enforce regime security. This encouraged the theory that the South African government have been prioritising the security of and stability of their rule over the country as opposed to taking cybercrime and security seriously. The South African 2015 Defence Review placed emphasis on the threat of cybercrime and its effects on national security. Cyber-attacks were classified into four categories: (a) cyber espionage, which involves gaining access to information without the permission of the data handler/ data subject, usually for commercial purposes (phishing); (b) malware, to commit identity theft, fraud, and extortion; (c) cyber warfare, which is an attempt by a state to direct offensive cyber operations to another stage or organisation/ company; (d) cyber terrorists, which are actions taken in cyberspace intended to harm a state, organisation or civilians (Griffiths, 2017).

Critique

Like many other laws and policies, the National Cybersecurity Policy Framework was partly the result of diffusion, drawing on sources such as the EU, the North Atlantic Treaty Organisation (NATO), and the U.S., which are more advanced users of technology and have faster-moving policy formulation (Gilardi, 2010 & Sutherland, 2017). According to Sutherland, "The South African government used some foreign experiences and texts, raising questions about the effectiveness of its adaptation to the legal and political systems and cultures, and the degree to which it has designed something it had the administrative and technological skills to deliver," (2017: 87).

Internationally, South Africa has supported a series of resolutions of the UN General Assembly (2010) concerning CSIRTs, protection of CNIs, and more generally, the work of the UN Office on Drugs and Crime (UNODC, 2017). It has also supported the International Multilateral Partnership Against Cyber-Terrorism (IMPACT), created by a UN official, but now seemingly defunct. At the 2017 ITU World Telecommunications Development Conference, attempts to amend Resolution 45 (Rev. 2014) on cybersecurity failed, due to wildly differing aims amongst countries. South Africa signed the Budapest Convention on Cybercrime (Council of Europe, 2001), but never ratified it. It has also signed, but not ratified, the African Union Convention on Cyber Security and Personal Data Protection (AU, 2014); indeed so few countries have ratified it that it is unlikely to come into force.

As a signatory to the International Covenant on Civil and Political Rights (ICCPR), South Africa is subject to periodic review, though it was 14 years late in submitting its most recent report (Sutherland, 2017: 92). Amongst many suggestions to South Africa from the UN Human Rights Committee (2016):

> The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act. It is also concerned about the wide scope of the data retention regime under the Act. The Committee is further concerned at reports of unlawful surveillance practices, including mass interception of communications carried out by the National Communications Centre, and at delays in fully operationalising the Protection of Personal Information Act, 2013, due in particular to delays in the establishment of an information regulator (arts. 17 and 21).

From the foregoing, the democratic South Africa has been consistent in its passive defence approach to issues of cybersecurity policies, and framework. It leverages on safeguarding local infrastructures and deterrence policies against criminals. However, the fallout to the liberal approach is the bureaucratic bottleneck made manifest in the process of plausible compliance with fundamental rights, democratic values, and carrying along of all relevance political institutions. In the circumstance, not much of success has been recorded in deterring cybercriminals and enhancing national security. The framework and cybersecurity strategy are still unfolding despite phenomenally high threat rate. Because, a lot of citizens, organisation, and several government institutions are falling prey to shrewd cyber criminals as more of the population embrace digital resource, and its opportunities. These dangers, combined with a large portion of the South African population that has not had regular or sustained exposure to technology and broadband internet access, expose local communities to cyber threats (Grober & van Vuuren *et al*, 2014).

Conclusion

South Africa's experience with cyber threats mirrors global trends but is influenced by its specific socio-economic and technological landscape. As the most economically vibrant country in Africa, it has both high internet penetration and significant exposure to cyber threats. The frequent attacks, such as the notable scams involving the South African Revenue Service and fake World Cup offers, emphasize the prevalence and impact of cybercrimes in the country.

Most cyber-attacks in South Africa have been attributed to foreign hackers, exploiting the country's relatively advanced internet infrastructure for malicious purposes. This situation not only affects individuals through scams and banking fraud but also poses broader security challenges for both public and private sectors. Cyber threats and crimes continue to evolve, driven by changes in technology, shifts in hacker tactics, and the varying levels of cybersecurity awareness and preparedness across different regions. While some incidents capture public and media attention due to their scale or novelty, others, like phishing, persist as consistent threats. The situation in South Africa exemplifies the complex interplay of local and international factors influencing cyber security. It underscores the need for robust, adaptable cybersecurity strategies that can address both the current threats and anticipate emerging challenges.

References

Barend Hendrik Pretorius, "Cyber-security and Governance for Industrial Control Systems," (master's dissertation., University of KwaZulu-Natal, 2016).

Brett van Niekerk, "An Analysis of Cyber-Incidents in South Africa," *The African Journal of Information and Communication* 20, no.20 (December 2017):114, https://doi.org/10.23962/10539/23573.

De Wet Potgieter," Absa Intercepts Land Bank Swindle," Saturday Star, 8 January 2011, http://www.iol.co.za/business/companies/absa-intercepts-land-bank-swindle-1.1009423.

Douglass Cecil North, *Institutions, Institutional Change and Economic Performance*(Cambridge: Cambridge University Press, 1990), 1-159.

Ewan Sutherland, "Governance of Cybersecurity: The Case of South Africa," The African Journal of Information and Communication 20, no.20(December 2017): 84, https://doi.org/10.23962/10539/23574.

Geoffrey Hawker, "Challenges for Parliament in South Africa*," Australian Parliamentary Review* 22, no.1(April 2007): 97-113.

Geoffrey Hawker, "Missing cadres? Listing Voting and the ANC's Management of its Parliamentarians in the National Assembly, 1999-2003," *Journal of African Elections* 2, no.2 (October 2003):97-115, https://doi.org/10.20940/JAE/2003/v2i2a7.

Harold Patrick, "Security Information Flow in the Public Sector: KZN Health and Education," (PhD thesis., University of KwaZulu-Natal, 2015).

Jan Andress, Steve Winterland,eds.*, Cybercrime Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2014(Waltham: Elsevier, 2014).

Joel Chigada, "Toward an Aligned South Africa National Cybersecurity Policy Framework" (PhD thesis., University of Cape Town, 2023), http://hdl.handle.net/11427/38253.

Mbongwa, Makua, "Moroccan Hackers Blamed for Website Blitz," *IOL News*, 13 January 2005, http://www.iol.co.za/news/south-african/moroccan-hackerss-blamed-for-website-blitz-231419.

Michael, J. Sodaro, *Comparative Politics: A Global Introduction*(New York: McGraw-Hill, 2004), 31.

Nir Kshetri, "Cybercrime and Cybersecurity in Africa," *Journal of Global Information Technology Management* 22, no.2(April 2019): 77-81, https://doi.org/10.1080/1097198X.2019.1603527.

Norton South Africa, "2012 Norton Cybercrime Report," 2012, http://za.norton.com/cybercrimereport/promo?inid=ukhhodownloadshomelinkcybercrimereport.

Pokwana, Kyobe, *Investigating the Mis-alignment in the Existing E-Legislation of South Africa*, 38.

SABC News, "Cyber-attacks reaching a critical point in South Africa," 19 April 2017, http://www.timenews.co.za/in-sa-wednesday-19-april-2017.

Siyabonga Mkhwanazi, "Roads Agnecy Account Hacked for R8.5.m.," *IOL News*, 12 October 2015, https://www.iol.co.za/capetimes/roads-agency-account-hacked-for-r8.5m-1.1928834.

Thennix Roux, "Constitutional Courts as Democratic Consolidators: Insights from South Africa After 20 Years," *Journal of Southern African Studies* 42, no.1(January 2016): 5-18, https://doi.org/10.1080/03057070.2016.1084770.

Virginia Braun, Victoria Clarke, "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology* 3, no.2(January 2006): https://doi.org/10.1191/1478088706qp063oa.

"African Union," *African Union Convention on cyber security and personal data protection*, adopted 27 June 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

"South African Government," *Minister David Mahlobo: State security Department Budget Vote 2015/16*, accessed April 2024, www.gov.za/news/speeches/minister-david-mahlobo-state-security-dept-budget-vote-201516-05-may-2015.

Christine Greyvenstein, "Aarto Website latest hacking victim," ITWeb, 24 April 2013, www.itweb.co.za/articles/aarto-web-site-latest-hacking-victim/3mYZRXv93zNMOgA8.

Deloitte, *Outsourcing is good for job creation in South Africa*, (Johannesburg: Deloitte & Touche, 2015).

Jerry Brito, Tate Watkins, "Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy," *Harvard National Security Journal* 3, no.1 (December 2011): 39-84, http://harvardnsj.org/2011/12/loving-the-cyber-bomb-the-dangers-of-threat-inflation-in-cybersecurity-policy/.

O' Keeffe v Argue Printing & Publishing Company Ltd, 1954(3) SA 244 (C).

RDM News Wire, "One in 10 SA businesses has experienced cyber attack in past year, *Sowetan Live*, 03 November 2015, http://sowetanlive.co.za/news/2015-11-03-one-in-10-sa-business-has-experienced-cyber-attack-in-past-year/.

UN Human Rights Commission, *CCPR/C/IAF/Z0/1: Concluding observations on the initial report of South Africa*, (Geneva: Office of the High Commissioner, 2016).

Van Vuuren, Grobler, Leenen, Phahlamohlaka, *Proposed model for a cybersecurity centre of innovation for South Africa*, (Heidelberg: Springer-Verlag, 293-306. https://doi.org/10.1007/978-3-662-44208-1_24

Suggested reading

De Lanerolle, 1. (2016). "Internet Freedom: Why Access Is Becoming a Human Right." http://theme diaonline.co.za/2016/06/intemet-freedom-why-access-is-beconiing-ahuman-right/

Gcaza, N. & von Solms, R. (2017). "A Strategy for A Cybersecurity Culture: A South African Perspective," *The Electronic Journal of Information Systems in Developing Countries,* 80(6): 1—17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Lewis, C. (2015). "SA Ranks High in Cybercrime." www.sabc.co.za/news/a/ebe2b3004a2f054d9f61dfa53d9712ffi/SA-ranks-high-in-cybercrime-20151012 Lotz, B. (2015). "We Don't Have Enough People to Cope with Cybercrime," *Hawks. Cybersecurity News,* www.htxt.co.za/2015/09/10/we-dont-have-enoughpeople-to-cope-with-cybercrime-hawks/ SA Government Gazette. (2015). "National Cybersecurity Policy Framework for South Africa." von Solms, R. & van Niekerk, J. (2013). "From Information Security to Cyber Security," *Computers & Security, 38:* 97-102.

References

Africa, S. (2012). "The Policy Evolution of the South African Civilian Intelligence Services: 1994 to 2009 and Beyond," *Strategic Review for Southern Africa,* 34(1): 97—134.

amaBhungane Centre for Investigative Journalism NPC and Stephen Patrick Sole v Minister of Justice and Correctional Services and 9 other respondents. (2019). Case no.: 25978/17, High Court of South Africa, Gauteng Division, Pretoria.

Bramwell, L. (2017, August 21). "Department of Telecommunications and Postal Services: Cybersecurity," Research Unit, Parliament Portfolio Committee of Telecommunications and Postal Services.

Burbidge, M. (2019, May 29). "Can SA Survive a Cyber Attack?" *IT Web*. www.itweb.co.za/content/mQwkoM6Kayeq3r9A

Centre for Constitutional Rights. (2017, August 10). "Concise Submission on the Cybercrimes and Cybersecurity Bill [B 6-2017]."

Donnelly, L. (2018, June 22). "Another Day, Another Data Breach," *Mail and Guardian.*

Duncan,J. (2015). *The Rise of the Securoaats: The Case of South Africa.* Johannesburg: Jacana.

Dunn Cavelty, M. (2016). "Cyber-Security," in A. Collins (ed.), *Contemporary Security Studies* (4th ed. pp. 400-416). New York: Oxford University Press.

Ferreira, E. (2019). "National Assembly Approves Critical Infrastructure Protection Bill, IOL News." www.iol.co.za/news/politics/national-assembly-approves-critical-infrastructure-protection-bill- 19647155

Gereda, S. L. (2006). "The Electronic Communication and Transactions Act," in L. Thornton, Y. Carrim, P. Mtshaulana & P. Reyburn (eds.), *Telecommunications Law in South Africa* (pp. 262-294). Johannesburg: STE Publishers.

Grobler, M., van Vuuren, J. J. & Leenen, L. (2011). "Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward," in M. D. Hercheui, D. Whitehouse, W. Mclver & J. Phahlamohlaka (eds.), *1CT Critical Infrastructures and Society* (pp. 215-225). HCC 2012. IF1P Advances in Information and Communication Technology, Vol. 386. Berlin and Heidelberk: Springer. https://doi.org/10.1007/978-3-642-33332-3_20

ISPA. (2015). "Submission on the Draft Cybercrime Cybersecurity Bill 2015." https://ispa.org.za/wp- content/uploads/2012/06/20151130-ISPA-Submission-on-the-Draft-Cybercrime-Cybersecurity- Bill-2015.pdf

ITU. (2008, April). "Overview of Cybersecurity: Recommendation ITU-T X.1205," Geneva, Switzerland. www.itu.int/rec/T-REC-X.1205-200804-I Luiijf, E., Besseling, K. & de Graaf, P. (2013). "Nineteen National Cyber Security Strategies," *International Journal of Critical Infrastructures,* 9(1/2): 3-31. https://doi.org/10.1504/IJCIS.2013.051608

Mangena, D. (2016). "Will Legislation Protect Your Virtual Space? Discussing the Draft Cybercrime and Cyber Security' Bill," *De Rebus, 560:* 33—34.

Mare, A. & Duncan, J. (2015). "An Analysis of the Communications Surveillance Legislative Framework in South Africa," Media Policy and Democracy Project, www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdt Maurer, T. (2011). "Cyber Norm Emergence at the United Nations - An Analysis of the UN's Activities Regarding Cyber-security," Discussion Paper 2011-11, Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

Media Monitoring Africa, MMA. (2018). Inquiry into the role and responsibilities of the Independent Communications Authority of South Africa in cybersecurity: Submissions by Media Monitoring Africa on the discussion document. 30 November 2018. https://www.icasa.org.za/uploads/files/ MMA-submission-discussion-document-on-cybersecurity.pdf Mzekandaba, S. (2019, June 27). "Top-level UN Human Rights Role Gives Tlakula Extra Digital Power," *IT Web.* www.itweb.co.za/content/wbrpOMgPlrgqDLZn Newmeyer, K. P. (2015). Elements of National Cybersecurity Strategy for Developing Nations," *National Cybersecurity Institute Journal,* 1(3): 9—19.

O'Brien, K. A. (2011). *The South African Intelligence Services: Front Apartheid to Democracy, 1948—2005.* New York: Routledge.

Olivier, B. (2013, July 28). "Is There a Need for Cyber-ethics?" *Mail and Guardian.* https://thoughtle ader.co.za/bertolivier/2013/07/28/is-there-a-need-for-cyber-ethics/

O'Reilly, K. (2013). "South African Law Coming to Grips with Cyber Crime," *De Rebus 530:* 14—15. Orji, U. (2012). *Cybersecurity Law and Regulation.* Nijmegen: Wolf Legal Publishers.

Pillay, V. (2014, September 2). "IEC Chair Pansy Tlakula Resigns." *Mail and Guardian.*

Privacy International. (2019). "The State of Privacy in South Africa." https://privacyintemational.org/ state-privacy /1010/state-privacy-south-africa

Right2Know Campaign. (2015, November 30). "Preliminary Position on the Draft Cybercrimes and Cybersecurity Bill."

Right2Know Campaign. (2017, August 10). "Cybercrimes, Cybersecurity, and Internet Freedom: Right2Know Campaign Submission on the Cybercrimes and Cybersecurity Bill."

RSA. (2010). "Draft Cyber Security Policy of South Africa," *Annex to Government Gazette,* 536(32963): 4-12.

RSA. (2010a). "Annual Report of the Joint Standing Committee on Intelligence for Financial Year Ending 31 March 2010." Parliament ATC.l 10921.

RSA. (2013, November 26). "Department of Communication Review Report: E-commerce, Cybercrime and Cybersecurity - Status, Gaps and the Road Ahead."

RSA. (2013a). "Ministerial Review Commission on Intelligence (Matthews Commission)."

RSA. (2014). *South African Defence Review 2014*. Pretoria: Government Printer.

RSA. (2015a). "State Security Agency, Notice Number 609 of 2015," *Government Gazette,* 609(39475): 67-95.

RSA. (2015b). "Address by Dr. Siyabonga Cwele, Minister of Telecommunications and Postal Services at the Launch of the Cybersecurity Hub at CS1R," Pretoria, South Africa, www.gov.za/speeches/ minister-siyabonga-cwele-launch-cybersecurity-hub-30-oct-2015-0000 RSA. (2017, February 28). "Department of Telecommunications and Postal Services (DTPS), Cybersecurity Briefing to the Portfolio Committee of Parliament."

RSA. (2017a). "Department of Justice and Constitutional Development Memorandum on the Objects of Cybercrimes and Cybersecurity Bill."

RSA. (2017b). *Department of Defence Annual Performance Plan for 2017*. Pretoria: Government Printer.

RSA. (2018). *Department of Defence Annual Performance Plan for 2018*. Pretoria: Government Printer. Sabillon, R., Cavalier, V. & Cano, J. (2016). "National Cyber Security Strategies: Global Trends in Cyberspace,'' *International Journal of Computer Science and Software Engineering,* 5(5): 67—81.

SAHRC. (2017, August). "Submission on the Cybercrimes and Cybersecurity Bill [B 6-2017].''

SANEF. (2019, June 4). "SANEF Supports Landmark Constitutional Challenge to South Africa's Surveillance Law, RICA." https://sanef.org.za/sanef-supports-landmark-constitutional-challenge-to- south-africas-surveillance-law-rica/

SAPA. (2013, October 15). "Carrim Announces New Cyber Security Council." *Mail and Guardian.* Schonteich, M. (2014). "A Story of Trials and Tribulations: The National Prosecuting Authority, 1998—2014." *SA Crime Quarterly* 50: 5—15. doi: 10.4314/sacq.v50il.l Snail, S. (2009). "Cyber Crime in South Africa — Hacking, Cracking, and Other Unlawful Online Activities*Journal of Information, Dun & Technology, 1:* 1—13. https://doi.org/10.4314/sacq.v50i1.1

Sole, S. (2019, September 18). "Analysis: Inside amaBhungane's Landmark Ruling on Surveillance," *Daily Maverick,* www.dailymaverick.co.za/article/2019-09-18-analysis-inside-amabhunganes-land mark-ruling-on-surveillance/

Sutherland, E. (2017). "Governance of Cybersecurity — The Case of South Africa," *The African Journal of Information and Communication, 20:* 83—112.

UCT. (2019, May 24). "Africa First for UCT Cybersecurity." www.news.uct.ac.za/article/-2019-05- 24-africa-first-for-ucts-cybersecurity

Wassemian, H. & de Beer, A. (2005). "Which Public? Whose Interest? The South African Media and Its Role during the First Ten Years of Democracy," *Critical Arts,* 19(1—2): 36—51. https://doi.org/10.1080/02560040585310041