Governance of Cybersecurity – The Case of South Africa

Ewan Sutherland
Visiting Adjunct Professor, LINK Centre, University of the Witwatersrand (Wits), Johannesburg

Abstract

Cybersecurity is a growing concern for governments, with the push for universal access to the Internet, the increasing ubiquity of social networks and the growing reliance on digital government service, and given a growing range of threats from foreign powers, terrorists and criminals. These complex issues span all government ministries, their agencies and contractors, plus provincial and municipal government, and require the state to create legal frameworks and agencies to protect data and offer advice to businesses and citizens, plus ensuring a sufficient supply of skilled technicians and engineers. In the case of South Africa, its government responded in 2015 with a National Cybersecurity Policy Framework (NCPF), with implementation led by the Ministry of State Security. The Protection of Personal Information (POPI) Act of 2013 created the Information Regulator to ensure data privacy. The POPI regime is only being implemented slowly and has overly wide exemptions for national security. South Africa lags behind advanced economies in cybersecurity legislation, in government coordination, in engagement with business and citizens, and in the supply of skilled labour. Delays have meant it lacks the experiences obtained in faster moving countries, and the improvements they have made to their policies and, especially, implementation. Parliament has neither pressed the government for faster action nor explored areas where powers might have been taken that infringe human rights.

Keywords
cybercrime, cybersecurity, data protection, privacy, governance, South Africa

DOI: https://doi.org/10.23962/10539/23574

Recommended citation

Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 83-112.
https://doi.org/10.23962/10539/23574

1. Introduction

National governments are adopting cybersecurity strategies to address a wide range of threats (OECD, 2012), including foreign governments attacking critical national infrastructure (CNI) (e.g., the electricity grid in Ukraine (Zetter, 2016)), criminals locking then ransoming computer systems (e.g., a hospital in England (Palmer, 2017)), hacktivists protesting against the activities of firms (e.g., Armscor (Moyo, 2016a; 2016b)) and the bulk theft of identities (Romanosky, Telang, & Acquisti, 2011). Such threats are of growing significance, given the pursuit by governments of universal Internet access and the rising use of and reliance on online government and commercial services, plus the ubiquity of social networks, and the emergence of an Internet of Things (IoT) that raises questions over the cybersecurity of objects as mundane as fridges and toys.[1] The governance challenges that follow from this include coordinating cybersecurity activities and data protection across the whole of government, including sub-national levels (e.g., municipalities), independent agencies (e.g., regulators), and contractors (e.g., outsourced services) (Chertoff, 2008). Governments must also influence the practices of businesses, especially CNI providers, as well as voluntary organisations, households, and individuals. Despite some national cybersecurity strategies having been reviewed and revised, there remain considerable challenges in ensuring these are well-constructed, cost-effective, and subject to appropriate governance (OECD, 2015; Dean, 2016). This article considers the governance of cybersecurity in South Africa, a complex federal state with a relatively sophisticated economy (OECD, 2017), though with many impoverished citizens (StatsSA, 2017), who often have limited digital literacy (RIA, 2016; Siemens, 2016), creating significant challenges for its government in assessing the risks from and of devising responses to:

- cybercrime;
- cyberespionage;
- cyberterrorism; and
- cyberwarfare.

In 2012, the South African Cabinet adopted a National Cybersecurity Policy Framework (NCPF, setting out measures and mechanisms for coordination across government (SSA, 2015). At the time of writing, the Information Regulator (i.e., the data protection authority) was not fully operational and the Cyber Warfare Strategy had yet to be finalised. The proposed coordination mechanisms were complex, making their management difficult, especially given the poor track record of inter-ministerial coordination and the difficulties in overcoming rivalries. Moreover, there are only limited oversight and review mechanisms, with many activities clouded in, possibly unnecessary and counterproductive, secrecy.

[1] There has been one major distributed denial of service (DDoS) attack using hacked closed-circuit television (CCTV) cameras (Goodin, 2017), while one government has issued a warning against use of particular toys (Conradis, 2017), and in one country, an adult toy manufacturer settled litigation over violations of the privacy of its customers (Roberts, 2017).

There are significant challenges in assessing possible threats and in keeping such assessments accurate, given advances in technologies and in their uses, such as the evolving "dark net" (Fachkha & Debbabi, 2016; Lacson & Jones, 2016), and the growing offensive capabilities of a few countries and of groups of individuals, including terrorists (Liff, 2012; Lindsay, 2015), plus a great many everyday cybercriminals (Akamai, 2016; 2017; Cisco, 2017). South Africa has been the country most often attacked in Africa (Wolfpack, 2013; TMG Digital, 2016; Van Heerden, Von Soms, & Mooi, 2016), with an estimated cost in 2014 of ZAR5.8 billion (Fripp, 2014). While one in 10 businesses reported a cyberattack during 2015, this is expected to rise significantly from 2018, when reporting is, finally, made mandatory, triggering much greater attention to prevention and security, especially because firms can then be held legally liable (Jonker, 2015). Cybercrimes are likely to be underreported by citizens, given their uncertainty about the capability of the South African Police Service (SAPS) in matters of technology. 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).

The African National Congress (ANC) has been in government since 1994, following the first elections under universal franchise (Southall, 1994). However, it has been losing its attractiveness to the electorate, as a result of internal rifts and its failures on service delivery, with President Zuma having emphasised loyalty to himself (Booysen, 2015; Southall, 2015; Paret, 2016). There is an independent and powerful Constitutional Court, one that has shown it will hold anyone and everyone to account (Gibson, 2016; Roux, 2016). Whereas Parliament has often struggled to scrutinise complex legislation and exercises only limited oversight of budgets, ministers and policies (Hawker, 2003; 2007). This 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. 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.

After 1994, 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. Nonetheless, section 198 of the 1996 Constitution, on the governance of the intelligence services, expressly controls what is now the State Security Agency (SSA), requiring it to observe the rights of citizens (Klaaren, 2015). Whether those rights are protected and the extent to which the SSA prefers to practice its own exceptionalism, believing that it is above rather than under the

Constitution, are matters of contention (Nathan, 2010; Van der Westhuizen, 2013). The only authoritative inquiry found that officials drafting and vetting operational policies lacked an adequate understanding of the Constitution and its protections for citizens (Matthews, Ginwala, & Nathan, 2008). A major concern has been that the SSA has become an instrument of senior members of the ANC, concerned more with its internal personal and political battles than with assessing and countering external and terrorist threats (Solomon, 2012; McKinley, 2013).[2] This has been further complicated by the fusion of the ANC with the state, the party having been in office for over two decades, deploying its own members into all levels of the administration, and emphasised by President Zuma having formerly been a head of the ANC intelligence service.

Assessing the relative performance of South Africa is limited by the lack of comparative data. Following its development of other compound indicators, the International Telecommunication Union produced the Global Cybersecurity Index (GCI) (ITU, 2017), with a view to raising awareness of the challenges.[3] The title is disingenuous, since the GCI measures not cybersecurity, but legislative measures and policies on paper, which do not determine and cannot predict levels of cybersecurity in practice. To measure cybersecurity it would be necessary to capture the efforts of governments and their agencies to implement and enforce the policies, for example, to identify budgets, campaigns, and skills development. Unsurprisingly, the "leading" nations in the GCI are OECD countries with good governance, plus a couple of the faster moving autocracies, while South Africa is considered "maturing", along with a mixed bag of countries. Commercial reports on cybersecurity point to realities as experienced by citizens and firms, but offer little specific information about South Africa (Akamai, 2016; 2017; Cisco, 2017; Microsoft, 2017; Norton, 2016; Symantec, 2017).

The challenges for businesses include legal liability for the loss of customer data and the consequential falls in share prices, loss of brand value and of customer loyalty (e.g., the Equifax data breach (Volz & Shepardson, 2017), and the release of 30 million South African IDs (Lotz, 2017)). Firms are often reluctant to admit to data breaches because of potential financial losses, despite such reporting being included in corporate social responsibility (CSR) and in some countries being a legal obligation under data protection laws, notably in South Africa from 2018. The King Committee (2016) called for the governing bodies of South African firms to be proactive in monitoring and responding to cyberattacks, though there has been no assessment of the effectiveness of corporate cybersecurity governance.

[2] Cyril Ramaphosa, despite being Deputy President, was apparently spied on because of his candidacy for the ANC Presidency (Letsoalo, 2017).

[3] One of its partners in this venture is the Egyptian regulatory authority that runs a deep packet inspection system for the repressive regime of Marshal Al Sisi.

The next section examines the National Cybersecurity Policy Framework. This is followed by analyses of privacy and data protection. Surveillance is then examined, insofar as information is made public, followed by an analysis of cybersecurity skills. Finally, conclusions are drawn and issues identified for further research.

2. The National Cybersecurity Policy Framework (NCPF)

Like many other laws and policies, the National Cybersecurity Policy Framework was partly the result of diffusion (Meseguer, 2005; Gilardi, 2010), drawing on sources such as the EU, the North Atlantic Treaty Organisation (NATO) and the US, which are more advanced users of technology and have faster-moving policy formulation (Grobler, Van Vuuren, & Leenen, 2012; Van Vuuren, Phahlamohlaka, & Leenen, 2012; 2014). 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.

The development of the NCPF was slow, not helped by President Zuma moving responsibility between Cabinet "clusters" and between departments, nor by his rapid turnover of ministers. The Minister of Communications published a detailed cybersecurity policy draft (Nyanda, 2010), which took two years to be approved by Cabinet and a further three years to be published, and only in Afrikaans and English.[4] By then, it was the Minister of State Security who was in charge (SSA, 2015), with the State Security Agency (SSA) responsible for implementing the policy, roadmap and strategy. Nonetheless, the Department for Telecommunications and Postal Services (DTPS), inheritor of part of the work of the Department of Communications (DoC), retained significant responsibilities.

Implementation of the NCPF requires extensive coordination across government (see Table 1), with the lead assigned to the Justice, Crime Prevention and Security Cluster of ministers (JCPS, n.d.). A Cybersecurity Response Committee, chaired by the Director-General of State Security, with the heads of the relevant departments and agencies, was charged with strategy and decision-making, and required to identify and prioritise areas for intervention, based on assessments of possible threats.[5] The closeness to state security means there is only limited transparency or oversight, though DTPS (2017a) did give an initial briefing to its Parliamentary Portfolio Committee. One weakness was that the national e-government strategy had not been updated for many years (DPSA, 2001), until the recent addition of a complementary strategy, strangely this came from DTPS, based on the ECT Act (DTPS, 2017b; 2017d). It admitted significant failures in implementing the 2001 policy and added some limited security measures, notably a Security Sub-Committee

[4] There are nine other official languages.

[5] The Cybersecurity Response Committee is supported by the SSA Cybersecurity Centre.

of the National e-government Steering Committee, though it failed to mention the NCPF.[6]

Table 1: Departments directly engaged in cybersecurity (RSA, 2016)

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	-	-

* Additionally, the various provinces have adopted their own e-government strategies.

[6] It maintained the 1996 Minimum Information Security Standards (MISS) ensuring "the national interests of the Republic are protected".

The overarching objective of government is (RSA, 2010a):

> Outcome 3: All people in South Africa are and feel safe.

Based on this, there was a "delivery agreement" between the Presidency and the Justice Ministerial Cluster (RSA, 2010b), calling for:

> Development of a Cybersecurity Policy and the implementation thereof.
> Development of capacity to combat and investigate cyber crime.

Nonetheless, the ability to combat and investigate breaches of cybersecurity seems to lie much further in the future, as does the prosecution of individuals, given the need to implement the Cybercrimes and Cybersecurity Bill and to train police, prosecutors and judges.

Formerly, the Department of Communications (DoC) sat in the Economic Sectors Ministerial Cluster, responsible for the communications regulatory authority and for broadcasting, posts and telecommunications markets. In 2014, the DoC was split, with the creation of the new Department of Telecommunications and Postal Services (DTPS), under a former security minister, taking over its work on cybersecurity. A National Cybersecurity Advisory Council (NCAC) had been created to aid the DoC on policy and technical issues (see Table 2), but is reported as having done very little (IT News Africa, 2013).[1] Nonetheless, in 2017 applications were invited to serve on a new NCAC (DTPS, 2017c).

Table 2: National Cybersecurity Advisory Council (Oxford, 2013)

Name	*Affiliation*
Barend Taute (Chairman)	Council for Scientific and Industrial Research (CSIR)
Ritasha Jethva (Vice-chairman)	Accenture
Dr Khomotso Kganyago	Chief Security Advisor, Microsoft South Africa (deceased 2014)
Prof Tana Pistorius	Department of Mercantile Law, University of South Africa (UNISA)
Mark Heyink	Attorney
Sizwe Snail	Attorney
Collen Weapond	Fraud and corruption specialist Advocate

Chapter XII of the Electronic Communications and Transactions (ECT) Act of 2002 provides for the establishment of a Cyber Inspectorate, with power to inspect, search, and seize content, in pursuit of the unacceptable. It was intended to assist law enforcement agencies, and to provide services directly to the public and businesses. No implementing regulations were ever promulgated, no Cyber Inspectors were appointed, and no offences created by Chapter XIII were ever prosecuted.

In the US, one organisational solution to widespread cyberattacks was the creation by government and by the private sector of Computer Security Incident Response Teams (CSIRTs) (Wiik, Gonzalez, & Kossakowski, 2006; Bronk, Thorbruegge, & Hakkaja, 2006; Grobler & Bryk, 2010). This followed the isolated and uncoordinated responses to the "Morris worm" or "Internet worm" in 1988, which was seen as having been poorly handled, with duplicated efforts and conflicting solutions. The US Defense Advanced Research Projects Agency (DARPA) established the Computer Emergency Response Team (CERT*) Coordination Center, setting a pattern replicated by many organisations and governments. The various CSIRTs soon began ad hoc exchanges of information, formalised from 1990 through the Forum for Incident Response and Security Teams (FIRST, n.d.; Gonzalez, 2005; Wiik & Kossakowski, 2005), including significant numbers of face-to-face meetings. Three South African CSIRTs participate in FIRST:

- First National Bank;
- government (ECS-CSIRT); and
- Standard Bank Group.

In 2015, DTPS launched the National Cybersecurity Hub (NCH, n.d.)), aimed at informing business, voluntary organisations and the public, and to serve as the national CSIRT, a contact point for both domestic and foreign CSIRTs (Cwele, 2015).

Like other countries, South Africa adopted a variety of approaches to e-government at national, provincial and municipal levels, purportedly all under the Department of Public Service and Administration (Trusler, 2003; Mutula & Mostert, 2010; Cloete, 2012; DPSA, n.d.; Mawela, 2017), 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.

The 2010 draft NCPF acknowledged the lack of coordination within government and the insufficiency of existing legal measures needed to counter and prosecute cybercrime. It aimed 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.

Organisational deficiencies were to be reduced by creating NCAC (see Table 2), with officials drawn from a range of ministries and agencies, and with five independent members, to coordinate implementation of policies. It was to work with the government CSIRT, responding to breaches, incidents, and threats though there is very little evidence it has yet done anything.

A central challenge for government is the promotion of cybersecurity measures amongst:

- government (at national, provincial and municipal levels);
- general public;
- private sector (both domestic and foreign firms);
- civil society; and
- special interest groups.

The Minister of Justice and Correctional Services (2015) published a draft Cybercrimes and Cybersecurity Bill in 2015, inviting comments, and later announced that a revised version was to be laid before Parliament (Minister of Justice, 2017b). However, it failed to publish either the comments received or an analysis of their content, making it impossible to know the extent to which the Department had responded to concerns, criticisms and proposals from experts and the general public. At the time of writing, the Bill is being scrutinised by the Portfolio Committee on Justice and Correctional Services (2017), which invited public comments and held two days of public hearings.[7] The Bill will formally create the Cyber Response Committee to coordinate work across government.

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).[8] It has also supported the International Multilateral Partnership Against Cyber-Terrorism (IMPACT, n.d.), created by a UN official, but now seemingly defunct. At the 2017 ITU World Telecommunications Development Conference, attempts to amend Resolution 45

[7] To date these have not been published, though the Department responded to them.

[8] UNODC has built up a repository of national laws and policies for cybersecurity.

(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),[9] South Africa is subject to periodic review, though it was 14 years late in submitting its most recent report. 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 operationalizing the Protection of Personal Information Act, 2013, due in particular to delays in the establishment of an information regulator (arts. 17 and 21).

A major part of any cybersecurity strategy concerns the military and its ability both to remain fully operational while under cyberattack and its capability to launch conventional and cyberattacks. The NCPF sets out the following tasks for the Department of Defence:

- address national security threats in cyberspace;
- combat cyberwarfare, cybercrime and other cyber ills;
- develop, review and update existing substantive and procedural laws to ensure alignment; and
- build confidence and trust in the secure use of information and communication technologies.

The preferred military terminology is information warfare, covering a broad range of operations in what it terms the "InfoSphere".

A Cyber Warfare Strategy is said to be at an advanced stage of development, having been submitted to the Chief of the South African National Defence Force (Department of Defence, 2016; 2017; Mapisa-Nqakula, 2016). In financial year 2016/17, there was to be a Cyberwarfare Implementation Plan and in 2017/18 a

[9] https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

Cyberwarfare Command Centre Headquarters, the latter delayed because of financial constraints:

> South Africa requires the protection of its cyber-domain, through (inter alia) a comprehensive information warfare capability, integrated into its intelligence-related information systems at the international, national and defence levels. Both defence and wider-government capabilities must be enhanced to secure vital networks. (Department of Defence, 2015a, p. vi)

The Department of Defence (2015b) offers very little indication of possible threats or of their likely origins. It seems unlikely that any country would attempt to conquer South Africa or to seek to carve off part, but some states might wish to destabilise its government (e.g., in retaliation for its involvement in other African states) or to attack its ruling political party. Some individuals and commercial groups might consider attacks that would affect the supply of minerals to the global market and thus their prices. However, the most obvious attacks appear likely to come from domestic opponents of the regime or well-financed groups engaged in corruption.[10]

A somewhat unusual twist in the organisational arrangements is that protection of state information against a cyberthreat is the primary responsibility of the State Security Agency through a private company, Electronic Communications Security (Pty) Ltd (COMSEC Pty Ltd). This company was established in 2002, with the primary purpose of ensuring that critical electronic communications are secure and protected.

Defence networks are targets for attacks because they run command and control, administration, personnel, logistics and finance information systems. These networks thus require protection, including the use of technologies not available on the open market:

> The department will focus on cyber security over the medium-term through the approval of a DOD Cyber Warfare Strategy in the FY2015/16 and establishing a Cyber Command Centre Headquarters by the FY2018/19. The latter will be executed in the Defence Intelligence budget programme at a projected cost of R511 million over the medium-term. (Department of Defence, 2015b, p. 56)

There are significant path dependencies from past decisions that limit the ability of government to craft its strategies and plans, and little evidence of international cooperation or peer review. The division of responsibilities between several government departments, whose ministers have changed relatively frequently, creates problems, noticeably in delays and in redundant or vestigial bodies. Rapid turnover

[10] For example, the Gupta family, through Oakbay, engaged an expensive public relations firm from the UK, spending sums that, had they been used for cyberattacks, could have been extremely damaging.

in ministers, reconfigurations of departments and complex coordination make it unnecessarily difficult for government to develop expertise and to deliver results, similar problems of turnover in committees make parliamentary oversight much more difficult.

3. Privacy and data protection

Unusually for Africa, South Africa has a common law right of privacy that dates from the 1950s (Burchell, 2009; Roos, 2016). A radio broadcaster consented to the publication of her photograph in a newspaper article, but the photograph was subsequently used in advertising without her consent, which was held to violate her right to privacy (O'Keeffe v Argus Printing, 1954).[11] The courts have also recognised unreasonable intrusions to include bugging a room, intercepting a telephone call, reading private documents, and unauthorised testing of blood. Some violations of privacy have been treated as criminal invasions of privacy (i.e., *crimen injuria*).

The Constitution of 1996 protects privacy in section 14:

> 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"?

Debates on security have heavy historical baggage, especially in respect of the long rule of the National Party, which imposed the pass laws that still colour any consideration of identity documents (Breckenridge, 2005; Donovan, 2015).[12] A proxy for a national identity database was created by the mandatory registration of all SIM cards, which now encompasses most citizens and residents and large numbers of visitors. Such databases are especially attractive to hackers seeking financial rewards

[11] The arguments echoed *Tolley v JS Fry & Sons Ltd* [1931] UKHL 1 (23 March 1931), http://www.bailii.org/uk/cases/UKHL/1931/1.html

[12] The US government has incorporated biometric identities into passports for its own citizens, and requires visitors to have either a biometric passport or a biometric visa (including fingerprints).

from stealing large and inclusive sets of personal details. There are serious doubts about the security of such databases, notably the loss of Terabytes of data from the US National Security Agency (NSA) (Reuters, 2017).[13]

South Africa has prepared data protection legislation, though on a peculiarly tortuous path (Roos, 2016):

- South African Law Reform Commission (SALRC)
    - included in work programme in 2000
    - published a paper on privacy and data protection (SALRC, 2003)
    - published a paper on data protection (SALRC, 2005)
- Protection of Personal Information Bill in 2009
- Protection of Personal Information (POPI) Act of 2013
    - signed by President (2013)
    - appointment of board member of the Information Regulator (Gallens, 2016).

At the time of writing, the POPI Act is not fully implemented and may not be until late 2018. It will enable citizens, as data subjects, to bring civil actions against firms for data breaches. 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 POPI Act 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; Nelson Hall, 2015; BPESA, n.d.).

A central question concerning data protection emerges from section 6(1)(c) of POPI, which excludes processing by or on behalf of a public body involving national security, defence or public safety. This appears to give 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.

[13] This included hacking tools.

In time South Africa should have a strong data protection law protecting privacy, combined with common law and the constitutional protections of privacy, though this might take a number of years. For the present, the intelligence services appear exempt, unless and until litigation is brought to limit their actions.

4. Surveillance

The interception of telephone calls has featured prominently in the South African popular press, because of the "spy tapes" concerning the then Deputy President Jacob Zuma and corruption allegations in the arms deal scandal (Wolf, 2011; 2015; *Zuma v DA*, 2017). The interception of postal articles and telephone calls was originally authorised by a minister, then from 1992 by a judge (Cohen, 2001), and since 1996, has been subject to the Constitution and its protection of human rights (see Table 3). The last are limited by national security, defined in the General Intelligence Law Amendment Act of 2013 (GILAA), to include the protection of the people and the territorial integrity of the Republic against the threat of or use of force, as well as espionage, sabotage and terrorism.

Table 3: Interception laws in South Africa

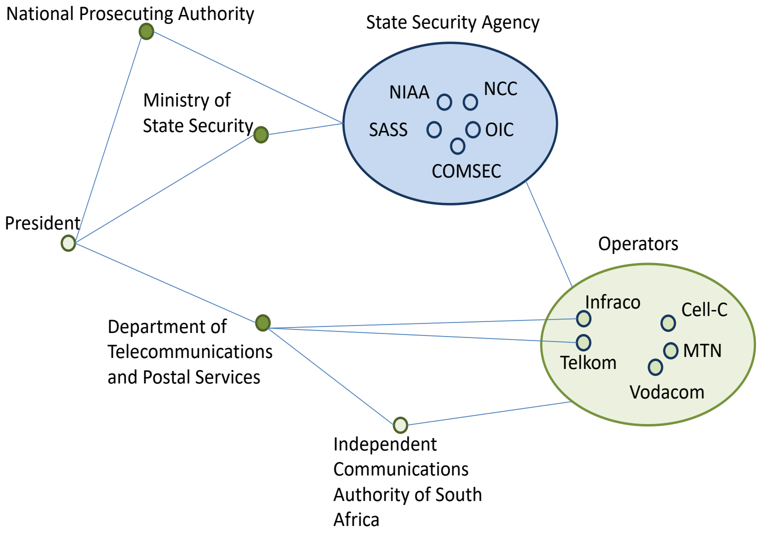
Statute	*Year*	*Section(s)*	*Authorisation*
Post Office Act	1958	118A	Minister
Interception and Monitoring Prohibition Act	1992	1	A discharged judge designated by the Minister of Justice
Interception and Monitoring Prohibition Amendment Act	1995	1	Redefines a judge to include currently serving, discharged and retired judges of the Supreme Court
Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA)	2002	7 & 8	A judge designated by Minister of Justice

All state intelligence activities are governed by the National Strategic Intelligence Act of 1994, Intelligence Services Oversight Act of 1994, Intelligence Services Act of 2002, and GILAA of 2013, stipulating that covert intelligence-gathering may only legally be conducted by these agencies. The Safety Matters Rationalisation Act of 1996 repealed 34 controversial apartheid-era laws dealing with security legislation, though it left significant security laws untouched.

The Intelligence Services Oversight Act of 1994 created the parliamentary Joint Standing Committee on Intelligence (JSCI, n.d.; Minister of Justice, 2017) and an

Inspector-General for Intelligence to investigate complaints, based on a framework set out in a white paper (RSA, 1994).[14] The JSCI comprises members of the six largest political parties in Parliament, charged with scrutinising and reporting on the finances and operations of the SSA (Ahmed, 1999). There are two routes for a citizen to complain about surveillance: to the JSCI or the Inspector-General. Nonetheless, there is considerable secrecy about surveillance practices, with sporadic attention from investigative journalists, non-governmental organisations (NGOs) and university researchers. There have also been a critical report by Privacy International (2016) and the suggestions by the UN Human Rights Committee (see above).

Figure 1: Surveillance system in South Africa


National Prosecuting Authority
State Security Agency
Ministry of State Security
NIAA
NCC
SASS
OIC
COMSEC
President
Operators
Infraco
Cell-C
Telkom
MTN
Vodacom
Department of Telecommunications and Postal Services
Independent Communications Authority of South Africa

The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) of 2002 created:

- the Office for Interception Centres (OIC); and
- the National Communications Centre (NCC).

The former is domestic, while the latter provides bulk monitoring and the interception of signals outside the country or passing through or entering South Africa (see Figure 1) (Watney, 2015; McKinley, 2016). RICA requires owners of mobile phones to register their SIM cards with their service providers, which have to obtain certain customer details and pass these on to the OIC. The OIC and NCC provide call data records (CDRs) and interception for the intelligence services, the National Prosecuting Authority (NPA) and Financial Intelligence Centre (FIC).

[14] The 1996 report of the JSCI covered the first wire-tapping scandal: the NIA tapping of the SAPS.

Related to the global adoption by businesses of CSR reporting, some service providers and network operators have published transparency reports on government collection of data and requirements to remove content from the Internet (GNI, n.d.)). The first transparency report by the Vodafone Group (2014) stated it was forbidden from publishing the scale of lawful interception on its network in South Africa.

Judge Yvonne Mokgoro was designated to approve and oversee applications from authorities seeking to intercept calls, on which she is required to publish annual reports (Mokgoro, 2014).[15] These have been intermittent, with the most recent report, covering 2014-15 (see Table 4), omitting any mention of IMSI-grabbers and limited to conventional interception. Her reports are sent to the parliamentary JSCI, which publishes them and considers their contents, though in closed meetings without publishing any minutes (JSCI, 2017; Minister of Justice and Corrctional Services, 2017). The only available JSCI report is minimalist, with no reference to cybersecurity (JSCI, 2015).

According to the Review Commission (Matthews, Ginwala, & Nathan, 2008), and subsequent investigative journalism, the NCC has mass surveillance capabilities unregulated by law, which would necessarily be unconstitutional. Twice the Ministry has introduced legislation that sought to recognise the NCC in law; in the first instance the National Strategic Intelligence Amendment Bill was withdrawn, in the second instance the relevant provisions were removed during parliamentary deliberations.

A further concern is the unregulated use by FIC, the SSA, and the South African Police Service (SAPS) of IMSI-grabbers,[16] devices that appear to be base stations belonging to mobile operators but which collect handset and SIM card details at a distance, with some allegedly able to perform man-in-the-middle attacks in order to intercept calls and data. One of these was used to jam mobile signals in Parliament (*Primedia Broadcasting v Speaker*, 2016), and another was found in a shopping mall in most peculiar circumstances.

While there are constitutional and legal frameworks for surveillance, these appear to be more honoured in the breach than in the observance, with the policies and practices for use of IMSI-grabbers protected from disclosure under the Promotion of Access to Information (PAI) Act,[17] and reporting by operators of requests for customer data prohibited by statute. The interceptions that are reported appear to be remarkably few in number (see Table 4), given the high level of crime (Kynoch, 2005); in particular, there is a long and dishonourable tradition in South Africa of political assassinations and financially-motivated killings, some apparently based

[15] Judge Mokgoro noted the need to update the terminology in RICA.

[16] Also known as IMSI-catchers and stingrays.

[17] See, for example, Peekhaus (2014).

on the locations of mobile phones (Shaw & Thomas, 2016; Shaw, 2017; Johnson, 2017).[18] Consequently, there is very little evidence that oversight and scrutiny are effective.

Table 4: Applications for directions to intercept under RICA (Mokgoro, 2014, p. 15)

	State Security Agency	*South African Secret Service*	*South Africa Police Service*	*Financial Intelligence Centre*	*South African National Defence Force*	*Total*
Applications (new)	28	2	150	3	3	185
Re-applications	30	-	2	-	-	54
Amendments	34	-	8	-	1	5
Extensions	31	-	4	-	-	35
Amendments and extensions	13	-	18	-	-	31
Entry warrants	4	-	-	-	-	4
Section 11	66	-	-	-	-	66
Oral intercepts	2	-	-	-	-	2
Refused	5 *	-	-	-	-	5
Total	**215**	**2**	**202**	**3**	**4**	**387**

* No RICA confirmation

5. Skills

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. 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). A particular problem is the very large number of small- and medium-sized enterprises (SMEs), which have limited budgets and capacity to develop ICT skills, thus requiring support from government. A major underlying concern is that too many schools lack the equipment and teachers trained in computer science and ICTs, aggravated by pupils not having computers and broadband access at home. While university graduations in ICTs have grown, it is by much less than other courses, in part because ICT students are dropping out (Kirlidog, Van der Vyver, Zeeman, & Coetzee, 2016).

In recent annual surveys, the Joburg Centre for Software Engineering (JCSE)

[18] It was alleged that the then-Minister of Communications sought a contract killer to eliminate the Chairman of the Parliamentary committee investigating her for corruption (ENCA, 2013).

reported an acute shortage of skilled ICT workers in South Africa, with information security a leading issue for employers (Schofield, 2016). It concluded that the ICT industry could not wait for local, provincial and national governments to provide solutions, while tertiary education institutions did not possess the necessary responsiveness. Consequently, the ICT profession and sector would have to solve the "crisis" through their own initiatives.

Cybersecurity presents particular problems, with the need for skilled individuals in the defence and security sectors, in critical national infrastructure, and in banking and finance. The implementation of the POPI Act will require all firms to bolster their cybersecurity efforts, with additional staff and significant CPD, up to board level. Without a substantial increase in supply, the shortage of skills will persist, with skilled individuals likely to be attracted to organisations able to pay the most.

At a more general level, the public needs to be taught about dangerous and unsafe behaviours on the Internet (e.g., passwords and phishing). The failure to teach schoolchildren about online safety has already been acknowledged (Kritzinger, 2014).

The NCPF recognised that South Africa would lag behind and be increasingly vulnerable unless it developed the necessary skills, for which it relied on colleges and universities (SSA, 2015, p. 13). However, the support for research and training has been limited. The South African Cyber Security Academic Alliance (SACSAA, n.d.) comprises three groups:

- Nelson Mandela University (NMU):
    - Centre for Research in Information and Cyber Security (CRICS, n.d.);
- University of Johannesburg (UJ):
    - Centre for Cyber Security (CSI, n.d.);
- University of South Africa (UNISA):
    - Cyber Security Awareness (CSA, n.d.).

In 2015, SACSAA ran an awareness campaigns, warning of the dangers of cyberbullying, and a poster competition. Recently it has been silent and appears to be moribund. There are some commercial initiatives, notably a Deloitte Cyber Intelligence Center (CIC), part of its global network of such centres (Mbelli & Dwolatzky, 2016). The South African Banking Risk Information Centre (SABRIC, n.d.) is a collective effort by the banking sector, leveraging public and private partners.

While the vast majority of surveillance technology firms are based in China, Europe, the US and, especially, Israel, there appear to be two in South Africa (see Table 5), VASTech and iSolv Technologies, with VASTech having received funding from the South African government (PI, 2014). Additionally, Lightning Bird Logistics in Stellenbosch acts as an agent for the sale of IMSI-grabbers from the US firm Verint.

Exports of surveillance and wiretapping technologies to other African countries should be subject to controls through the South African National Conventional Arms Control Committee (NCACC), implementing the National Conventional Arms Control Act of 2000 and the international Wassenaar Arrangement (2017).

Table 5: Firms in South Africa engaged in surveillance technologies

Firm	*Location*	*Description*
VASTech (n.d.)	Technopark, Stellenbosch	An independent firm, established in 1999, selling hardware and software to government to be used in fighting cross-border and international crime.
iSolv Technologies(n.d.)	Parktown North, Johannesburg	A privately-owned company focused on the development and production of state-of-the-art ICT security solutions. Specialising in communications monitoring and cybersecurity.

As is the case more widely in ICTs, South Africa lacks sufficient skills for effective cybersecurity, with shortages affecting government recruitment and retention of staff. To date, efforts to engage the wider population for basic cybersecurity have received limited attention and resources.

6. Conclusions

A major complaint about the South African government has been its failure in service delivery, of which cybersecurity is an example, even if not widely appreciated. It has been the result of delays, of inadequate assessments of the risks, of insufficient transparency, and of difficulties in coordination across government, business and society. While the government has, somewhat tardily, adopted a National Cybersecurity Policy Framework, it is of considerable complexity and is being implemented only slowly, with very limited reporting and Parliamentary oversight. The various organisational structures and their links into yet more structures suggest that implementation will continue to prove difficult, with coordination essential between many rivalrous ministers, many of whom may soon move on. The lack of priority placed on cybersecurity is reflected in the policy taking two years to go from draft to adoption, the Cybercrimes Bill also taking two years, and similar delays with the Cyber Warfare Strategy. It will ultimately have taken two decades to deliver a data protection authority, depriving South Africa of the lessons that could have been learned in that time.

Parliamentary oversight is very difficult given the technical complexity of the material and the inter-ministerial spaghetti, aggravated by unnecessary turnover in committee membership, limiting the development of expertise. Surprisingly, there were no parliamentary inquiries into the failure of the cybercrime inspectorate provisions of the ECT Act, the cleaving of DTPS from DoC, or the misuse of IMSI-grabbers, unlike comparable inquiries in the EU, UK and US (PAC, 2017; GAO, 2017; Oversight Committee, 2016; Schwab, 2016). Given the importance of cybersecurity to human rights and to growth of the digital economy, Parliament needs to develop methods to address its cross-governmental and technical nature, for example, by creating a forum or panel of expert advisers, together with a mechanism for coordination between Parliamentary Portfolio Committees.

The NCPF appears to have been written without much consideration of implementation, echoing the confused complexity of the ICT White Paper (DTPS, 2016; Freedman, 2016; McLeod, 2017). While there has been diffusion of policy elements and ideas from Europe and the US, there is little evidence of these having been adapted to South African national circumstances, especially the absence of any public assessment of the risks or of the potential impact of the proposed measures, or consideration of the ability to implement. The government failed to publish its analyses of the responses to its drafts of law and policy, raising questions about how effectively it makes use of such material and pointing to a serious weakness in governance.

That the intelligence and police services have wiretapping capabilities is very clear, though there is little evidence this reduces crime rates or secures South Africa against terrorism. It is observed more from leaks and the illicit sale and use of data, than from an increased number of prosecutions or greater success in the courts. Indeed, petty corruption in the interception of calls and in access to databases appears to be a significant problem, though the individuals are seldom prosecuted. The use of IMSI-grabbers is even more opaque, apparently without a policy or legal basis, used for blocking mobile signals in the vicinity of the President and possibly deployed more widely and much more intrusively. Yet more disturbing is the use of surveillance malware by the State Security Agency and Financial Intelligence Centre, which would certainly be unconstitutional. Ordinarily, those should have prompted Parliament to inquire into the use of such intrusive technologies, more commonly used by repressive regimes such as those in Ethiopia or Uganda. The likely outcome is for NGOs to go to the Constitutional Court for definitive rulings on the limits of the use of national security as a justification to withhold policy documents requested under the PAI Act, and then for them to seek to limit the use of IMSI-grabbers and surveillance software in order to uphold rights to dignity and privacy.

A major challenge is to persuade individual citizens and families to adopt good practice for cybersecurity, which requires a mixture of education and publicity. To date, relatively little has been done or to have been planned by government or industry, despite the rising levels of Internet adoption and global concern about cyberthreats. A similar challenge lies in the persuasion of businesses, which must adopt appropriate measures to defend themselves, and the data they hold about their customers, from attacks, and to report all attacks that get through. This is an area in which the government needs to improve its credibility, by securing its own systems, by reporting its own breaches, and by helping and encouraging business to develop toolkits to defend themselves. These problems are aggravated by a longstanding shortage of ICT skills, which has hampered technology deployment and economic growth.

The diffusion and adaptation of cybersecurity policies requires further research, not least to determine the extent to which they are being matched to real threats and abilities, rather than being copied pro forma. It would also be useful to evaluate the effectiveness of coordination mechanisms within the South African Government, and with provincial and municipal administrations. An interesting phenomenon to monitor would be the spill-over of laws, policies and practices from South Africa into other SADC countries, and the ways in which they are adapted, rather than just being copied. The question of the availability of IMSI-grabbers is contentious and vexed, but requires work on their use by the Presidency, SSA, SAPS, criminals and, perhaps, foreign powers and terrorists. Equally, the use of surveillance malware requires further work, though this would be very difficult.

References

African Union (AU). (2014). Convention on Cyber Security and Personal Data Protection. Addis Ababa. Retrieved from https://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Ahmed, S. (1999). Being intelligent about intelligence: SA parliamentary oversight. *South African Journal of International Affairs, 6*(2), 191-198. https://doi.org/10.1080/10220469909545273

Akamai. (2016). *How the Mirai botnet is fuelling today's largest and most crippling DDOS attacks.* Cambridge, MA. Retrieved from https://www.akamai.com/uk/en/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf

Akamai. (2017). *State of the Internet/security Q4 2016 report.* Cambridge, MA. Retrieved from https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

Beresford, A. (2015). Power, patronage, and gatekeeper politics in South Africa. *African Affairs, 114*(455), 226-248. https://doi.org/10.1093/afraf/adu083

Booysen, S. (2015). *Dominance and decline: The ANC in the time of Zuma.* Johannesburg: Wits University Press.

Business Process Enabling South Africa (BPESA). (n.d.). Website. Retrieved from http://www.bpesa.org.za/

Breckenridge, K. (2005). The biometric state: the promise and peril of digital government in the new South Africa. *Journal of Southern African Studies, 31*(2), 267-282. https://doi.org/10.1080/03057070500109458

Brito, J., & Watkins, T. (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *Harvard National Security Journal, 3*(1), 39-84. Retrieved from http://harvardnsj.org/2011/12/loving-the-cyber-bomb-the-dangers-of-threat-inflation-in-cybersecurity-policy/

Bronk, H., Thorbruegge, M., & Hakkaja, M. (2006). *A step-by-step approach on how to setup a CSIRT.* Heraklion: European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/csirt-setting-up-guide

Burchell, J. (2009). The legal protection of privacy in South Africa: A transplantable hybrid. *Electronic Journal of Comparative Law, 13*(1), 1-26. Retrieved from http://www.ejcl.org/131/art131-2.pdf

Chertoff, M. (2008). The cybersecurity challenge. *Regulation & Governance, 2*(4), 480-484. https://doi.org/10.1111/j.1748-5991.2008.00051.x

Cisco. (2017). *Annual cybersecurity report.* San Jose, CA. Retrieved from http://www.cisco.com/c/en/us/products/security/security-reports.html

Cloete, F. (2012). E-government lessons from South Africa 2001-2011: Institutions, state of progress and measurement. *The African Journal of Information and Communication (AJIC), 12,* 128-142. https://doi.org/10.23962/10539/19712

Cohen, T. (2001). "But for the nicety of knocking and requesting a right of entry": Surveillance law and privacy rights in South Africa. *South African Journal of Information and Communication (SAJIC), 1,* 1-18. https://doi.org/10.23962/10539/19841

Conradis, B. (2017, February 21). German regulator tells parents to destroy "spy" doll Cayla. *Deutsche Welle*. Retrieved from http://www.dw.com/en/german-regulator-tells-parents-to-destroy-spy-doll-cayla/a-37601577

Council of Europe. (2001). Convention on Cybercrime. *ETS No.185.* Strasbourg. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Centre for Research in Information and Cyber Security (CRICS). (n.d.). Website. Nelson Mandela University. Retrieved from http://crics.mandela.ac.za/

Cyber Security Awareness (CSA). (n.d.). Website. University of South Africa (UNISA). Retrieved from http://eagle.unisa.ac.za/elmarie/

Centre for Cyber Security (CSI). (n.d.).Website. Retrieved from http://adam.uj.ac.za/csi/

Corruption Watch (CW). (2016). *Annual report.* Johannesburg.

Cwele, S. C. (2015, October 30). Minister Siyabonga Cwele: Launch of Cybersecurity Hub. Text of speech. Retrieved from http://www.gov.za/speeches/minister-siyabonga-cwele-launch-cybersecurity-hub-30-oct-2015-0000

Dean, B. (2016). Natural and quasi-natural experiments to evaluate cybersecurity policies. *Journal of International Affairs, 70*(1), 139-160. Retrieved from https://jia.sipa.columbia.edu/natural-and-quasi-natural-experiments-evaluate-cybersecurity-policies

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

Department of Defence. (2015a). *South African defence review.* Pretoria. Retrieved from http://www.dod.mil.za/documents/defencereview/Defence%20Review%202015.pdf

Department of Defence. (2015b). *Department of Defence strategic plan for 2015 to 2020.* Pretoria. Retrieved from http://www.dod.mil.za/documents/annualreports/DoD%20Annual%20Performance%20Strat%20Plan%202403.pdf

Department of Defence. (2016). *Annual report 2015/16*. Pretoria. Retrieved from http://www.gov.za/sites/www.gov.za/files/DoD_Annual_Report_2015-2016%20RGB.pdf

Department of Defence. (2017). *Annual performance plan*. Pretoria. Retrieved from http://www.dod.mil.za/documents/app/2017/DoD%20APP%202017%20web%2010%20March.pdf

Department of Public Service and Administration (DPSA). (2001). *Electronic government: The digital future: A public service IT policy framework*. Pretoria.

DPSA (2012). *Public service corporate governance of information and communication technology policy framework*. Pretoria. Retrieved from http://www.gov.za/sites/www.gov.za/files/CGICTPolicyFramework.pdf

DPSA. (n.d.). Website. Retrieved from http://www.dpsa.gov.za/

Donovan, K. P. (2015). The biometric imaginary: Bureaucratic technopolitics in post-apartheid welfare. *Journal of Southern African Studies, 41*(4), 815-833. https://doi.org/10.1080/03057070.2015.1049485

Department of Telecommunications and Postal Services (DTPS). (2016). *National Integrated ICT Policy White Paper*. *Government Gazette, 176*(40325). Retrieved from http://www.gov.za/sites/www.gov.za/files/40325_gon1212.pdf

DTPS. (2017a). Cybersecurity: Department & SABRIC briefing, with Deputy Minister present. Retrieved from https://pmg.org.za/committee-meeting/24042/

DTPS. (2017b). *National e-government strategy and roadmap: Digitizing government services*. *Government Gazette, 622*(40772).

DTPS. (2017c). Invitation to nominate members of the National Cyber Security Advisory Council. Retrieved from https://www.dtps.gov.za/index.php?option=com_content&view=article&id=703:national-cybersecurity-advisory-council&catid=51:popular-topics&Itemid=298

DTPS. (2017d). *National e-Government Strategy and Roadmap*. *Government Gazette, 629*(41241).

EFF v Speaker of the National Assembly, ZACC 11 (Constitutional Court March 31, 2016).

Electronic Communications Security - Computer Security Incident Response Team (ECS-CSIRT). (n.d.). Website. Retrieved from http://www.ssa.gov.za/CSIRT.aspx

ENCA. (2013, August 12). Answers wanted in alleged Pule assassination plot. Retrieved from https://www.enca.com/south-africa/pule-linked-alleged-assassination-plot

EU. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

EU. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Brussels. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Fachkha, C., & Debbabi, M. (2016). Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization. *IEEE Communications Surveys & Tutorials, 18*(2), 1197-1227. https://doi.org/10.1109/COMST.2015.2497690

Feinstein, A. (2010, June 7). Rise of the tenderpreneurs, the fall of South Africa. *New Statesman*. Retrieved from http://www.newstatesman.com/africa/2010/06/south-world-anc-party-zuma

Forum for Incident Response and Security Teams (FIRST). (n.d.). Website. Retrieved from https://www.first.org/

Freedman, M. (2016, October 10). South Africa: ICT white paper under fire. *Extensia.* Retrieved from http://extensia-ltd.com/south-africa-ict-white-paper-fire/

Fripp, C. (2014, November 11). Cybercrime costs South Africa about R5.8 billion a year. *htxt. africa.* Retrieved from http://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/

Gallens, M. (2016, October 26). Pansy Tlakula appointed as new information regulator. *News24.* Retrieved from http://www.news24.com/SouthAfrica/News/pansy-tlakula-appointed-as-new-information-regulator-20161026

Gibson, J. L. (2016). Reassessing the institutional legitimacy of the South African Constitutional Court: New evidence, revised theory. *Politikon: South African Journal of Political Studies, 43*(1), 53-77. https://doi.org/10.1080/02589346.2016.1155135

Gilardi, F. (2010). Who learns from what in policy diffusion processes? *American Journal of Political Science, 54*(3), 650-666. https://doi.org/10.1111/j.1540-5907.2010.00452.x

Global Network Initiative (GNI). (n.d.). Website. Retrieved from http://www.globalnetworkinitiative.org/

Gonzalez, J. (2005). Computer safety, reliability, and security. In R. Winther, B. A. Gran, & G. Dahll (Eds.), *24th International Conference, SAFECOMP 2005.* Cham, Switzerland: Springer. https://doi.org/10.1007/11563228

Goodin, D. (2017, February 27). *Record-breaking DDoS reportedly delivered by 145,000+ hacked cameras.* Ars Technica. Retrieved from https://arstechnica.co.uk/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

Government Accountability Office (GAO). (2017). *Cybersecurity – actions needed to strengthen U.S. capabilities. GAO-17-440T.* Washington, DC. Retrieved from http://gao.gov/products/GAO-17-440T

Grobler, M., & Bryk, H. (2010). Common challenges faced during the establishment of a CSIRT. In H. S. Venter, M. Coetzee, & M. Loock (Eds.), *Information security for South Africa (ISSA)* (pp. 1-6). New York: IEEE.
https://doi.org/10.1109/ISSA.2010.5588307

Grobler, M., Van Vuuren, J. J., & Leenen, L. (2012). Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward. In M. D. Hercheui, D. Whitehouse, W. McIver, & J. Phahlamohlaka (Eds.), *IFIP International Conference on Human Choice and Computers* (pp. 215-225). Berlin: Springer.
https://doi.org/10.1007/978-3-642-33332-3_20

Hawker, G. (2003). Missing cadres? List voting and the ANC's management of its parliamentarians in the National Assembly, 1999-2003. *Journal of African Elections, 2*(1), 97-115. Retrieved from http://journals.co.za/content/eisa_jae/2/2/EJC32346

Hawker, G. (2007). Challenges for parliament in South Africa. *Australasian Parliamentary Review, 22*(1), 97-113.

International Multilateral Partnership Against Cyber-Terrorism (IMPACT). (n.d.). Website. Retrieved from http://www.impact-alliance.org/home/index.html

International Telecommunication Union (ITU). (2017). *Global cybersecurity index.* Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

iSolv Technologies. (n.d.). Website. Retrieved from https://isolvtech.com/

IT News Africa. (2013, October 15). South Africa launches National Cyber Security Advisory Council. Retrieved from http://www.itnewsafrica.com/2013/10/south-africa-launches-national-cyber-security-advisory-council/

Johnson, R. W. (2017). *How long will South Africa survive? The crisis continues.* Johannesburg: Jonathan Ball.

Joint Standing Committee on Intelligence (JSCI). (n.d.). Website. Retrieved from http://www.parliament.gov.za/live/content.php?Item_ID=215&CommitteeID=132

JSCI. (2015). *Report of the Joint Standing Committee on Intelligence on activities of the Committee after 5 months of establishment.* Cape Town. Retrieved from https://pmg.org.za/tabledcommitteereport/

Jonker, M. (2015, November 2). One in ten SA businesses have experienced cyberattacks. Grant Thornton. Retrieved from https://www.grantthornton.co.za/insights/articles/one-in-ten-sa-businesses-have-experienced-cyber-attacks-in-the-past-year/

Justice, Crime Prevention and Security Cluster (JCPS). (n.d.). About. Retrieved from http://www.gov.za/about-government/justice-crime-prevention-and-security-cluster

King Committee. (2016). *King IV: Report on corporate governance.* Johannesburg: The Institute of Directors in Southern Africa.

Kirlidog, M., Van der Vyver, C., Zeeman, M., & Coetzee, W. (2016). Unfulfilled need: Reasons for insufficient ICT skills in South Africa. *Information Development*, 1-15. https://doi.org/10.1177/0266666916671984

Klaaren, J. (2015). The judicial role in defining national security and access to information in South Africa. *Democracy and Security, 11*(3), 275-297. https://doi.org/10.1080/17419166.2015.1067613

Koelble, T. (2017). One-party dominance and public sector corruption in South Africa: Consequences for democracy. In P. Harfst, I. Kubbe, & T. Poguntke (Eds.), *Parties, governments and elites* (pp. 281-300). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-17446-0_14

Kritzinger, E. (2014). Online safety in South Africa – a cause for growing concern. In H. S. Venter, M. Laack, M. Coetzee, & M. M. Elaf (Eds.), *Information Security for South Africa (ISSA) 2014.* New York: IEEE. https://doi.org/10.1109/ISSA.2014.6950502

Kynoch, G. (2005). Crime, conflict and politics in transition-era South Africa. *African Affairs, 104*(416), 493-514. https://doi.org/10.1093/afraf/adi009

Lacson, W., & Jones, B. (2016). The 21st century DarkNet market: Lessons from the fall of Silk Road. *International Journal of Cyber Criminology, 10*(1), 40-61. https://doi.org/10.5281/zenodo.58521

Letsoalo, M. (2017, September 8). "Spooks" cash "used to spy on Cyril Ramaphosa". *Mail & Guardian*. Retrieved from https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril

Liff, A. P. (2012). Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies, 35*(3), 401-428. https://doi.org/10.1080/01402390.2012.66325 2

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cyber Security, 1*(1), 53-67. https://doi.org/10.1093/cybsec/tyv003

Lotz, B. (2017, October 23). Your ID number is online – why that's bad and what you can do. *Mail & Guardian*. Retrieved from https://mg.co.za/article/2017-10-23-your-id-number-is-online-why-thats-bad-and-what-you-can-do

Mapisa-Nqakula, N. (2016, May 11). Minister Nosiviwe Mapisa-Nqakula: Defence and Military Veterans Dept Budget Vote 2016/17. Text of speech. Retrieved from http://www.gov.za/speeches/minister-nosiviwe-mapisa-nqakula-defence-and-military-veterans-dept-budget-vote-201617-11

Matthews, J., Ginwala, F., & Nathan, L. (2008). *Intelligence in a constitutional democracy: A report to the Minister for Intelligence Services.* Pretoria: Ministry of Intelligence Services.

Mawela, T. (2017). Exploring the role of social media in the G2C relationship: A South African perspective. *Information Development, 33*(2), 117-132. https://doi.org/10.1177/0266666916639743

Mbelli, T. M., & Dwolatzky, B. (2016). Cyber security, a threat to cyber banking in South Africa: An approach to network and application security. In M. Qiu, L. Tao, & J. Niu (Eds.), *IEEE 3rd International Conference on Cyber Security and Cloud Computing.* New York: IEEE Computer Society. https://doi.org/10.1109/CSCloud.2016.18

McKinley, D. T. (2013). State and civil-political rights in South Africa. *Strategic Review for Southern Africa, 35*(1), 118-134.

McKinley, D. T. (2014). Secrecy and power in South Africa. In G. M. Khadiagala, P. Naidoo, D. Pillay, & R. Southall (Eds.), *New South African review 4: A fragile democracy - twenty years on.* Johannesburg: Wits University Press.

McKinley, D. T. (2016). *New terrains of privacy in South Africa: Biometrics/smart identification systems, CCTV/ALPR, drones, mandatory SIM card registration and FICA.* Johannesburg: Right2Know Campaign & Media Policy & Democracy Project. Retrieved from http://www.r2k.org.za/2016/12/15/research-new-terrains-of-privacy-in-south-africa/

McLeod, D. (2017, January 25). ICT white paper "not constitutional". *TechCentral.* Retrieved from https://techcentral.co.za/ict-white-paper-unconstitutional/71367/

Meseguer, C. (2005). Policy learning, policy diffusion, and the making of a new order. *The Annals of the American Academy of Political and Social Science, 598*(1), 67-82.

Microsoft. (2017). *Microsoft security intelligence report*. Retrieved from https://www.microsoft.com/en-us/security/Intelligence-report

Minister of Justice. (2015). *[draft] Cybercrimes and Cybersecurity Bill.* Minister of Justice and Correctional Services. Retrieved from http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf

Minister of Justice. (2017). *Cybercrimes and Cybersecurity Bill.* Minister of Justice and Correctional Services. Retrieved from http://pmg-assets.s3-website-eu-west-1.amazonaws.com/CyberCrimes-Bill-2017.pdf

Mokgoro, Y. (2014). *Report on interception of private communications.* Cape Town: Parliament of the Republic of South Africa. Retrieved from http://pmg-assets.s3-website-eu-west-1.amazonaws.com/160127report.pdf

Moyo, A. (2016a, July 15). Armscor plays down hack. *ITWeb.*

Moyo, A. (2016b, July 25). Armscor beefs up security. *ITWeb.*

Mutula, S. M., & Mostert, J. (2010). Challenges and opportunities of e-government in South Africa. *The Electronic Library, 28*(1), 38-53. https://doi.org/10.1108/02640471011023360

Nathan, L. (2009). Lighting up the intelligence community: An agenda for intelligence reform in South Africa. *African Security Review, 18*(1), 91-104. https://doi.org/10.1080/10246029.2009.9627518

Nathan, L. (2010). Intelligence bound: The South African Constitution and intelligence services. *International Affairs, 86*(1), 195-210. https://doi.org/10.1111/j.1468-2346.2010.00875.x

National Cybersecurity Hub (NCH). (n.d.). Website. Retrieved from https://www.cybersecurityhub.gov.za

Nelson Hall. (2015). *Analysis of South Africa as a BPO delivery location.* Cape Town: Business Process Enabling South Africa (BPESA).

North, D. C. (1990). *The economics of public issues* (8th ed.). New York: Harper and Row.

Norton. (2016). *2016 Norton cyber security insights report*. Retrieved from https://uk.norton.com/cyber-security-insights

Nyanda, S. (2010, February 19). Notice of intention to make South African National Cybersecurity Policy. *Government Gazette, 536*(32963).

O'Keeffe v Argus Printing and Publishing Company Ltd [1954] (3) SA 244 (C).

Organisation for Economic Co-operation and Development (OECD). (2012). *Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy.* Paris.

OECD. (2015). *Digital security risk management for economic and social prosperity.* Paris.

OECD. (2017). *Economic survey of South Africa 2017.* Paris. Retrieved from http://www.oecd.org/eco/surveys/economic-survey-south-africa.htm

Oversight Committee. (2016). *Law enforcement use of cell-site simulation technologies: privacy concerns and recommendations.* Washington, DC: Committee on Oversight and Government Reform, US Congress. Retrieved from https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf

Oxford, A. (2013, October 16). Who's who on South Africa's new Cyber Security Advisory Council. *htxt.africa*. Retrieved from http://www.htxt.co.za/2013/10/16/whos-who-on-south-africas-new-cyber-security-advisory-council/

Palmer, D. (2017, February 1). Misconfigured firewall blamed for hospital ransomware infection. *ZDnet*. Retrieved from http://www.zdnet.com/article/misconfigured-firewall-blamed-for-hospital-ransomware-infection/

Paret, M. (2016). Contested ANC hegemony in the urban townships: Evidence from the 2014 South African election. *African Affairs, 115*(460), 419-442. https://doi.org/10.1093/afraf/adw025

Peekhaus, W. (2014). South Africa's Promotion of Access to Information Act: An analysis of relevant jurisprudence. *Journal of Information Policy, 4*, 570-596. https://doi.org/10.5325/jinfopoli.4.2014.0570

Portfolio Committee on Justice and Correctional Services. (2017). Have your say: The Cybercrimes and Cybersecurity Bill. Retrieved from https://www.parliament.gov.za/committee-notice-details/29

Primedia Broadcasting v Speaker (784/2015) [2016] ZASCA 142 (29 September 2016). Retrieved from http://www.saflii.org/za/cases/ZASCA/2016/142.html

Privacy International (PI). (2014, January 30). South African government still funding VASTech, knows previous financing was for mass surveillance. Retrieved from https://www.privacyinternational.org/node/305

PI. (2016). *State of privacy South Africa.* London. Retrieved from https://www.privacyinternational.org/node/968

Public Accounts Committee (PAC). (2017). *Protecting information across government. HC 769.* London: House of Commons. Retrieved from http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/publications/

Republic of South Africa (RSA). (1994). *White Paper on Intelligence.* Pretoria. Retrieved from http://www.gov.za/documents/intelligence-white-paper

RSA. (2006). Cryptography Regulations R.216. *Government Gazette, 489*(28594). Retrieved from http://www.gov.za/sites/www.gov.za/files/28594.pdf

RSA. (2010a). *Outputs and measures: Outcome 3: All people in South Africa are and feel safe*. Retrieved from https://www.gov.za/sites/default/files/outcome-3.pdf

RSA. (2010b). *Delivery agreement for outcome three: "All people in South Africa are and feel safe".* Pretoria.

RSA. (2016). Structure and functions of the South African government. Retrieved from http://www.gov.za/node/537988

Research ICT Africa (RIA). (2016). Submission to the Parliament of South Africa on "The cost to communicate in South Africa". Cape Town. Retrieved from http://www.researchictafrica.net/publications/Other_publications/2016_South%20Africa_Cost%20to%20Communicate%20Submission_RIA%20.pdf

Reuters. (2017, February 8). NSA contractor indicted over mammoth theft of classified data. Retrieved from http://www.reuters.com/article/us-usa-cybersecurity-nsa-contractor-idUSKBN15N2N4

Roberts, J. J. (2017, March 10). Sex toy maker pays $3.75 million to settle "smart" vibrator lawsuit. *Fortune*. Retrieved from http://fortune.com/2017/03/10/sex-toy-maker-settlement-smart-vibrator-lawsuit/

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*(2), 256-286. https://doi.org/10.1002/pam.20567

Roos, A. (2016). Data protection law in South Africa. In A. B. Makulilo (Ed.), *African data privacy laws* (pp. 189-227). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-47317-8

Roux, T. (2016). Constitutional courts as democratic consolidators: Insights from South Africa after 20 Years. *Journal of Southern African Studies, 42*(1), 5-18. https://doi.org/10.2139/ssrn.2501176

Schofield, A. (2016). *2016 JCSE ICT skills survey.* Johannesburg: Joburg Centre for Software Engineering (JCSE).

Schofield, A. (2017). *2017 JCSE ICT Skills Survey.* Johannesburg: Joburg Centre for Software Engineering (JCSE).

Schwab, A. (2016). *Recommendation for a second reading. A8-0211/2016.* Brussels: European Parliament. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0211+0+DOC+PDF+V0//EN

Shaw, M. (2017). *Hitmen for hire: Exposing South Africa's underworld.* Johannesburg: Jonathan Ball.

Shaw, M., & Thomas, K. (2016). The commercialization of assassination: "Hits" and contract killing in South Africa, 2000-2015. *African Affairs*, 1-24. https://doi.org/10.1093/afraf/adw050

Siemens. (2016). *African digitalisation maturity report 2017.* Munich. Retrieved from https://www.siemens.com/content/dam/internet/siemens-com/global/company/topic-areas/digitalization/pdf/survey/siemens-african-digitalization-report.pdf

Solomon, H. (2012). The demise of South Africa's intelligence community and the erosion of the liberal democratic state. *Africa Review, 4*(2), 157-172.

South African Banking Risk Information Centre (SABRIC). (n.d.). Website. Retrieved from https://www.sabric.co.za

South African Cyber Security Academic Alliance (SACSAA). (n.d.). Website. Retrieved from http://www.cyberaware.org.za/

South African Law Reform Commission (SALRC). (2003). *Privacy and data protection – issue paper.* Pretoria.

SALRC. (2005). *Privacy and data protection.* Pretoria. Retrieved from http://www.justice.gov.za/salrc/dpapers/dp109.pdf

Southall, R. (1994). The South African elections of 1994: The remaking of a dominant-party state. *The Journal of Modern African Studies, 32*(4), 629-655. https://doi.org/10.1017/S0022278X00015883

Southall, R. (2015). The coming crisis of Zuma's ANC: The party state confronts fiscal crisis. *Review of African Political Economy, 43*(147), 73-88. https://doi.org/10.1080/03056244.2015.1083970

State Security Agency (SSA) (2015). *The National Cybersecurity Policy Framework (NCPF). Government Gazette* (39475). Retrieved from https://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf

Statistics South Africa (StatsSA). (2017). *Poverty trends in South Africa: An examination of absolute poverty between 2006 and 2011, 2015.* Pretoria.

Symantec. (2017). *Internet security threat report*. Retrieved from https://www.symantec.com/security-center/threat-report

Times Live. (2016, January 25). Cyber-crime: SA the most targeted on the continent. Retrieved from http://www.timeslive.co.za/local/2016/01/25/Cyber-crime-SA-the-most-targeted-on-the-continent1

Trusler, J. (2003). South African e-government policy and practices: A framework to close the gap. In R. Traunmüller (Ed.), *Electronic Government. EGOV 2003* (pp. 504-507). Berlin & Heidelberg: Springer. https://doi.org/10.1007/10929179_95

Turok, B. (2017). South Africa's lopsided economy. *New Agenda: South African Journal of Social and Economic Policy, 2017*(65), 6-9. Retrieved from http://hdl.handle.net/10520/EJC-900a1510b

UN General Assembly. (2010). *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. A/RES/64/211.* New York. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

UN Human Rights Committee. (2016). *Concluding observations on the initial report of South Africa. CCPR/C/ZAF/CO/1.* Geneva.

UN Office on Drugs and Crime (UNODC). (2017). *Emerging crimes*. Retrieved from http://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html#Cybercrime

Van der Westhuizen, C. (2013). South Africa and national security. *Index on Censorship*, *42*(2), 62-64. https://doi.org/10.1177/0306422013494290

Van Heerden, R., Von Soms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa. In IEEE (Ed.), *IST-Africa Week Conference.* New York: IEEE. https://doi.org/10.1109/ISTAFRICA.2016.7530663

Van Vuuren, J. J., Phahlamohlaka, J., & Leenen, L. (2012). Governance of cybersecurity in South Africa. Paper presented at11th European Conference on Information Warfare and Security, Laval, France, 5-6 July. Retrieved from http://hdl.handle.net/10204/6207

Van Vuuren, J. J., Phahlamohlaka, J., Leenen, L., & Zaaiman, J. (2014). An approach to governance of cybersecurity in South Africa. In Information Resources Management Association (Ed.), *Cyber behavior: concepts, methodologies, tools, and applications* (pp. 1583-1597). Hershey: IGI Global. https://doi.org/10.4018/978-1-4666-5942-1.ch082

VASTech. (n.d.). Website. Retrieved from http://www.vastech.co.za/

Vodafone. (2014). *Law enforcement disclosure report*. Retrieved from http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

Volz, D., & Shepardson, D. (2017, September 8). Criticism of Equifax data breach response mounts, shares tumble. *Reuters*. Retrieved from https://www.reuters.com/article/us-equifax-cyber/criticism-of-equifax-data-breach-response-mounts-shares-tumble-idUSKCN1BJ1NF

Wassenaar Arrangement. (2017). *The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies*. Retrieved from http://www.wassenaar.org

Watney, M. (2015). State-on-nationals' electronic communication surveillance in South Africa: A murky legal landscape to navigate? In H. S. Venter, M. Loock, M. Coetzee, M. M. Eloff, & S Flowerday (Eds.), *Information Security for South Africa (ISSA)* (pp. 1-6). Johanesburg: IEEE. https://doi.org/10.1109/ISSA.2015.7335047

Wiik, J., & Kossakowski, K.-P. (2005). Dynamics of incident response. In FIRST (Ed.), *FIRST 2005* (pp. 1-24). Retrieved from https://first.org/conference/2005/papers/speaker14-paper-1.pdf

Wiik, J., Gonzalez, J. J., & Kossakowski, K.-P. (2006). Effectiveness of proactive CSIRT Services. Paper presented at Forum for Incident Response and Security Teams (FIRST), Baltimore, MD, 25-30 June 2006. Retrieved from https://www.first.org/conference/2006/papers/kossakowski-klaus-papers.pdf

Wolf, L. (2011). The prosecuting discretion: A power under administrative law or criminal law? *Tydskrif vir die Suid-Afrikaanse Reg, 2011*(4), 703-729.

Wolf, L. (2015). The National Prosecuting Authority (NPA) in a nimbus between the executive and the judicature. *Administratio Publica, 23*(4), 30-53.

Wolfpack. (2013). *2012/13 The South African cyber threat barometer.* Johannesburg. Retrieved from http://us-cdn.creamermedia.co.za/assets/articles/attachments/41981_sa_2012_cyber_threat_barometer_medium_res.pdf

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired.* Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zuma v DA (771/2016 & 1170/2016) [2017] ZASCA 146 (13 October 2017). Retrieved from http://www.saflii.org/za/cases/ZASCA/2017/146.html