The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet

Scott Timcke

Senior Research Associate, Research ICT Africa (RIA), Cape Town; and Centre for Social Change, University of Johannesburg

https://orcid.org/0000-0001-7125-8306

Mark Gaffley

PhD Candidate, Department of Private Law, University of Cape Town

https://orcid.org/0000-0001-8999-4221

Andrew Rens

Senior Research Fellow, Research ICT Africa (RIA), Cape Town

https://orcid.org/0009-0006-5877-983X

Abstract

Using South African state-owned enterprise (SOE) Transnet as a case study, this article explores the factors that influence the cybersecurity risks that are posed to infrastructure, with implications for markets and society, by advanced computational systems. We studied the legislation and corporate governance decisions leading up to the July 2021 breach of Transnet's IT network, a high-profile event with potential cascading consequences. We also examined the evolution, since the country's transition to democracy, of the South African government's approach to fostering a developmental state. The findings illustrate that cybersecurity policy needs to be a core dimension of contemporary South African socioeconomic development policy, necessitating a central role for the developmental state in creating trusted marketplaces and procuring suitable security software systems. The findings also underscore the reality that a failure to act against increasing cyber-threats constitutes a substantial risk to the functioning of the South African market. Based on the findings, this article argues for a close examination of how the cybersecurity performance of South African SOEs can be improved. While focused on South Africa, the findings are relevant to other countries seeking to integrate robust cybersecurity measures into their national logistical and infrastructural sectors.

Keywords

cybersecurity, cyber-incidents, state-owned enterprises (SOEs), developmental state, IT networks, Transnet, South Africa

Acknowledgements
The research informing this article was made possible by a grant to the Research ICT Africa (RIA) Just AI project from Canada's International Development Research Centre (IDRC) and the Swedish International Development Cooperation Agency (SIDA). We are grateful to Rachel Adams, Enrico Calandro, and Thuli Olorunju for their insights on working drafts, and to Charmaine Smith for editorial support. The article draws on elements of an April 2023 RIA Working Paper (Timcke et al., 2023).

DOI: https://doi.org/10.23962/ajic.i32.16949

Recommended citation
Timcke, S., Gaffley, M., & Rens, A. (2023). The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. *The African Journal of Information and Communication (AJIC)*, *32*, 1-28. https://doi.org/10.23962/ajic.i32.16949

1. Introduction

As we argue in this article, cybersecurity is a core matter for a country's socioeconomic development policy. Yet the literature on the connection between these two is still maturing. "When analysing the securitisation of countries' cyberspace, the empirical assessment of industrial policies is still rather unexplored", writes Tijerina (2022, p. 194). We are of the view that this deficit must be remedied if one views cybersecurity in relation to the political economy of inequality and risk (Timcke, 2023). These unequal risks affect citizens' livelihoods, meaning that cybersecurity issues cannot be treated as the exclusive domain of the state security cluster.

Transnet is a state-owned enterprise (SOE) in South Africa. The company is responsible for ports, rail, and pipelines and has a monopoly in bulk freight. To provide a sense of Transnet's strategic importance to trade flows in the South African economy, in 2021 nine commodities made up approximately 43% of the GDP, and contributed 80% of Transnet's revenue. The company has a property portfolio of ZAR35 billion (approx. USD2 billion), which includes industrial warehousing and commercial, retail, and residential property. Lockdowns during the global COVID-19 pandemic greatly impacted Transnet's revenue, which in 2021 was down 10.5% to ZAR67.3 billion (approx. USD3.94 billion) with a ZAR8.7 billion loss (approx. USD500 million). In 2022, revenue increased by 1.8% to ZAR68.5 billion with a net profit of ZAR5 billion, mostly coming from a 5.9% decrease in operating expenses via voluntary severance packages (Transnet, 2021a). Transnet's importance is even greater when considering indirect contribution, as most South African exports use its networks and facilities. This is why recent Transnet capacity problems have contributed to severe losses of export earnings in the agriculture and mining sectors, with an estimated annual loss of up to ZAR50 billion (approx. USD2.79 billion) for the coal, chrome, iron-ore and manganese sectors (Venter, 2022).

State monopolies have pros and cons, depending on their purposes. Chang (2007) summarises the literature on SOEs, stating that there "is no clear theoretical case either for or against SOEs" and there is "no clear systemic evidence that SOEs are burdens on the economy" (2007, pp. 7–8).[1] Whatever the view of SOEs, when these entities supply critical services, such as electricity, telecommunications, port, and rail infrastructure, they present singular vulnerability to cyber-incidents. A cyber-incident is an attempt to damage a computer network and/or IT system.

In response to a highly visible ransomware attack on Johannesburg's electricity supply in 2019 (BBC, 2019), South African analysts sought to raise awareness with government, key stakeholders, and citizens about the vulnerability of critical infrastructure. Efforts intensified in early 2021 (see, e.g., Allen, 2021a). A few months later, in July 2021, the Transnet cyber-incident occurred, with IT systems being unavailable for use at cargo terminals. This disruption added to global supply chain problems caused by the COVID-19 pandemic. The public was notified of the incident by the media, with Transnet issuing statements over the succeeding days. The company was not overly forthcoming about details at the time. Remarks were provided in annual reporting, with public investor relations presentations describing the event as "a cyber-attack, security intrusion and sabotage" which resulted "in the disruption of normal processes and functions" (Transnet, 2021a, p. 25).

SOEs play a significant role in the South African economy, and their prominence is expected to continue. Most SOEs provide infrastructure that is essential to the

[1] There is a view that outright rejects government ownership of any sort, claiming that SOEs perform poorly, make less profit, and are less efficient because the labour force is not sufficiently disciplined by market forces due to some degree of job tenure. The accumulation of these deficiencies leads, according to this view, to fiscal crises, with the state repeatedly having to bail out these entities. This view ignores the fact that SOEs might have other purposes and elements of value. Indeed, some SOEs exist to address market failures or to operate in sectors that are unlikely to ever be profitable and hence adequately served by private firms. SOEs are political entities, and their performance should be evaluated from the vantage point of the interplay between several agendas and competing objectives.

proper functioning of markets, and of society. By contrast, an individual commercial firm is not essential in this way, unless it has de facto monopoly of an essential service. Since SOEs are under control of the state, they are a significant means by which socioeconomic development policy can be realised, and from which failures of this policy may be determined. Existing estimates of costs from cybersecurity breaches in the South African economy should be viewed critically due to uncertainties about the included activities and calculation methods.[2]

As the July 2021 cyber-incident targeted an SOE, this article links general operational issues with larger governance issues. In South Africa, SOEs are guided by a developmental-state project (Mayedwa, 2018; Muller et al., 2015). Below we cover the history and politics of this project as it relates to cybersecurity, grounded in an understanding that developmental states are "driven by an urgent need to promote economic growth and to industrialise" and otherwise "catch up" with developed countries (Leftwich, 1996, p. 61). The project is both ideological and structuralist: "its major preoccupation is to ensure sustained economic growth and development on the back of high rates of accumulation, industrialisation and structural change" (UNCTAD, 2007, pp. 59–60), an undertaking that Sen (1999) argues is "a process of expanding the real freedoms that people enjoy" (1999, p. 36).

Much of what Sen (1999) refers to requires achieving economic development. Economic development is a qualitative shift in economic structure and in the social relationships to, and within, that structure. The bulk freight sector is a highly strategic one, capable of either inhibiting or facilitating economic development as well as the expansion of other domestic industries. The vibrancy of downstream industries is directly related to the efficiency of bulk freight. Therefore, the measures that Transnet takes to secure operations around logistics directly and indirectly impact the rest of the economy and the people who rely upon it. This is especially so when taking into account South Africa's aspirational digital industrialisation efforts and what this transformation could mean for the future alleviation of unemployment, inequality, and poverty.

Method and data sources

The main research method used in this study was process tracing. This method studies how "causal processes work using case study methods" (Beach, 2017, p. 1). The aim is to give "within-case analysis based on qualitative data" in a systematic fashion; indeed, "process tracing is a fundamental tool of qualitative analysis" (Collier, 2011, p. 823). Among the main data sources for process tracing in this study were the

[2] Some figures include ZAR50 billion in 2014 (Van Niekerk, 2017), ZAR43 billion in 2016 (Interpol, 2021), and ZAR5.7 billion in 2018 (Shaw, 2018). As a point of reference, in 2021, South Africa's GDP was about ZAR7 trillion (approx.. USD420 billion).

narratives of business performance in annual reports (Qian & Sun, 2021). Business performance is typically measured with standardised accounting indicators. Yet with risk management practices increasingly becoming components of annual reporting—as is the case in South Africa with the successive reports of the King Committee (IoDSA & King Committee on Corporate Governance, 2016)—there is scope to augment objective audited figures with the written judgements of executives and their management teams. Since we argue that cybersecurity policy needs to be a core dimension of contemporary socioeconomic development policy, a narrow forensic investigation into the precise details of how the attack was carried out (even if those details were available) or a recounting of the administrative details of how many cybersecurity staff were employed, their qualifications, and links to state security agencies, would be otiose. This is because inadequacies in this regard flow not merely from organisational failures to prioritise cybersecurity, but also from the policy environment, which failed to make it a priority or to hold Transnet accountable for it.

Narratives in annual reporting show how executives conceptualise past and future actions, and also give some indication of what actions they intend to take to safeguard the financial well-being of the business. Certainly, “narratives in corporate annual reports are intentionally manipulated by the informant”, yet overarching fiduciary requirements and auditory compliance do shape these narratives as well. This means that “these reports [can] help to uncover current, corporate operating conditions, and reveal future potential from the management point of view”, as well as revealing “rhetorical aspects of voluntary disclosure” (Qian & Sun, 2021, p. 1). We prioritised the study of Transnet’s annual reporting from 2009 to 2022, focusing on risk self-assessments to its IT systems (Transnet 2009a; 2010; 2011; 2012; 2013; 2014; 2015; 2016; 2017; 2018; 2019; 2020; 2021b; 2022).

Organisation

This article briefly examines the politics influencing the post-apartheid form of South African state and society, which shapes the governance of SOEs. These elements provide the contextual bedding for the latter half of the article, which presents a case study of the Transnet cyber-incident. It traces Transnet’s IT architecture plans over a decade, noting discrepancies between planning and actual investments and how executives sought to understand emerging threats introduced by new technologies, and it examines the board’s actions post-attack. The article concludes with discussion of the implications of cybersecurity for economic justice and commodity circulation in the developmental-state model.

2. South Africa's developmental-state model

It is beyond the scope of this study to comprehensively detail the intense three-decade-long politics between the state, capital, and labour (and factions within all three) over the structure and purpose of SOEs in post-apartheid South Africa. Still, a short contextual description can provide a useful primer on the considerations that led to the governance structures in Transnet, many of which continue to shape its operations.

When the African National Congress (ANC) formed the first democratically elected government in 1994, there were more than 700 SOEs (The Presidency, 2012, p. 67). A fair number of these enterprises existed due to duplication of functions in the "independent" Bantustans. With high popular expectations for democratisation to change material conditions, and trepidation by (white) capital around local investment due to the evolving dynamics of the period, the ANC initially viewed selective privatisation of SOEs as a means to reduce the state's debt. Another goal was to attract foreign direct investment by enhancing market confidence, signalling a policy shift away from nationalisation. More broadly, the main historical factors that curtail South Africa's development are massive social inequality as it relates to the trade-offs between growth and democratically guided redistribution (Gumede, 2009). Given these limiting factors, as well as the aforementioned reticence by local capital to invest, the developmental-state model advocates for the state to become a market actor, in order to eradicate poverty and attain humane, meaningful, and sustainable livelihoods (Thomas, 2000; World Bank, 2008).

Impressed with the economic performance of East Asian countries in the later stages of the 20th century, and taking heed of Malaysia's efforts to use the state and affirmative action policies to redress racial inequalities (Gumede, 2009), South African officials believed that the developmental-state model was the appropriate vehicle to build the material foundation for a well-functioning national democratic society. Ideas around the South African developmental state can be traced to a few sources, including the ANC's 1994 Reconstruction and Development Programme (ANC, 1994) and the 1996 Growth, Employment, and Redistribution (GEAR) macroeconomic policies (Department of Finance, 1996), and can also be extrapolated from the later chapters of the 1996 South African Constitution (Constitution of the Republic of South Africa, 1996). The developmental-state model was more clearly articulated in the South African government's successive Medium-Term Strategic Frameworks and in documents such as the National Development Plan 2030 and the 2012 *Report of the Presidential Review Committee on State-owned Entities* (The Presidency, 2012, pp. 34–35).

Like other areas of South African society formed during the transition to democratic rule in the 1990s, the developmental-state model was a product of the negotiated settlement and the pressures exerted by an international political economy enamoured with markets and championed by institutions like the World Bank and the International Monetary Fund (Fourie, 2022; Gumede, 2016; Southall, 2013). More broadly, the model aims to stoke capitalist development through active state-led policy while also entrenching a rights-respecting approach to public administration and state governance. The theoretical anchoring for this model comes from the work of Johnson (1982) and Evans (1995), amongst others. In recent years, the model has been supplemented by Mazzucato's (2013) research on the entrepreneurial state, which is an updated description of the benefits of state intervention in the market. President Cyril Ramaphosa appointed Mazzucato to the Presidential Economic Advisory Council in October 2019 (The Presidency, 2019), a signal that the developmental-state model remains at the forefront of thinking among many South African state officials, even if local academics are more circumspect about the state's performance and structure (e.g., Ukwandu, 2019) and the capability of SOEs to deliver this mandate (e.g., Gumede, 2016).

Turning from political economy debates to policy frameworks, the adoption of GEAR in 1996 as a macroeconomic strategy sought to provide guidance so that SOEs could become more efficient and provide effective services for the public (DPE, 2000). Given that the ANC relied heavily on organised labour movements to attain and maintain rule, massive unions such as the Congress of South African Trade Unions felt betrayed by the privatisation agenda (Gall, 1997). After taking strike action, organised labour signed the National Framework Agreement with the government in early 1996, which set out terms for restructuring on a case-by-case basis over a period of three years, taking into account the impact on workers.

Nevertheless, the government proceeded with restructuring SOEs, making provision for corporatisation, outsourcing to the private sector, and cost-recovery for public services. The ANC also undertook cadre deployment from the party to SOEs, a practice that every president in the democratic South Africa has defended despite continuous criticism. Black business groups encouraged privatisation, as the use of preferential procurement strategies by SOEs could create a black capitalist class. By contrast, labour was wary of the consequences of selling state property (Gumede, 2016). Indeed, it was only under Alec Erwin, the Minister of Public Enterprises (2004–2008), who displayed an appreciation for how the pursuit of private profit can clash with the pursuit of the public good, that SOEs faced these competing considerations (Erwin, 2004). Meanwhile, as restructuring unfolded over the next decade, repeated rounds of bailout, recapitalisation, and repositioning led to mass layoffs of labour, while outsourcing led to workers being unable to afford the very services that they had built and maintained. Barbara Hogan, the then-Minister of Public Enterprises (2009–2010), summed up the outcome as follows: the "disposal of non-core assets in the Transnet stable has enabled the corporation to focus on its core business" (Hogan, 2009).

Developmental-state theory requires the state to take the initiative to create the preconditions for development, in particular by increasing human capital and technical capacity. In South Africa, this requires addressing the disparate access to developmental preconditions. The role of SOEs is to ensure that developmental preconditions are met for those for whom market provision is inadequate. Due to the centrality of information and communication technology (ICT) systems to social and economic life, safety from cybercrime is, in the contemporary era, a precondition for development. Cybersecurity is thus a developmental priority. While dedicated cybersecurity capacity within the central state and up-to-date legislation are essential, neither will suffice to develop sufficient human capital or technical capacity to provide cyber safety. In South Africa, SOEs are required to develop human capital and technical capacity for the economy. As a result, cybersecurity is not simply an operational necessity but a policy priority.

3. Overview of cybersecurity incidents with economic effects in South Africa

Known cyber-incidents

As shown in Table 1, Van Niekerk (2017) identified 54 documented cyber-incidents between 1994 and 2016 in South Africa (see Van Heerden et al. (2016) for classification schema).

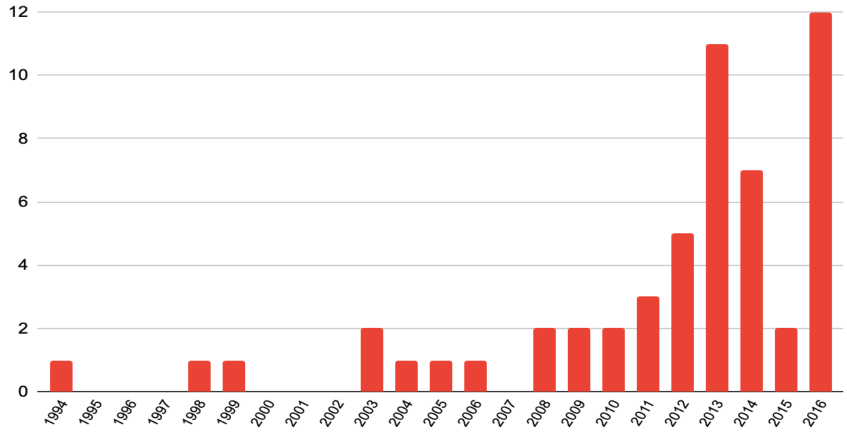
Table 1: Documented cyber-incidents, 1994–2016

Incident type	Number
Data exposure	22
Financial	12
Denial of service	9
Defacement	8
Data corruption	2
System penetration	1
Total	**54**

Note. Data sourced from Van Niekerk (2017).

There were only three cyber-incidents prior to 2002, with most happening from 2003 onwards, and with a surge in the later years (see Graph 1). The main perpetrators were hacktivists (17 incidents) and criminals (11 incidents). Nation-states were perpetrators in five instances, although Van Niekerk (2017) does not provide details on identity, targets, or type of incidents for this class. Of the 54 incidents, the targets were nearly equally split between state and private entities. Pieterse (2021) updates these figures to 2020, finding that there were 19 cyber-incidents in 2020. In Pieterse's 10-year review (2010–2020), the author found that nearly 40% of cyber-incidents were related to data exposure, about 21% related to compromised websites, and about 15% were cases of systems intrusion. This research has heuristic merit, but one limitation of this data is that it cannot show the severity or scale of these incidents. Defacing a political party's website is different from phishing to acquire financial passwords, which is different from a nation-state penetrating a government system, for example. That there is a dearth of statistics, especially from the state, to supplement those given here is indicative of the fact that cybersecurity has not been appreciated as core to South African socioeconomic development policy.

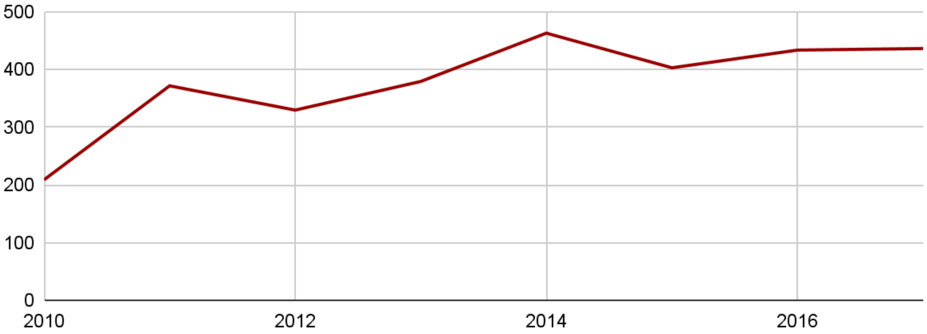
Figure 1: Frequency of documented cyber-incidents in South Africa



***Note*.** Date sourced from Van Niekerk (2017).

Within the same period of Van Niekerk's research, the banking industry experienced a rise in credit card fraud (see Graph 2). This activity prompted banks to put in place risk-detection and prevention systems, by increasing the rollout of chip and PIN systems (SABRIC, 2012).

Figure 2: Fraud loss on SA-issued credit cards, 2010–2017



***Note*.** Data sourced from SABRIC (2017).

During the course of 2018, the South African Banking Risk Information Centre (SABRIC) found that cybercrime took advantage of new banking products and services as customers were familiarising themselves with banking apps. "As with cybercrime, card fraud has seen a dramatic increase as criminals find new ways of accessing client card data", and "mostly through social engineering" (SABRIC, 2018, p. 4). SABRIC began publicly reporting digital crimes in 2017. As Table 2 shows, there was a 74% increase in the costs of digital crime between 2017 and 2021, with the number of incidents also rising.

Table 2: Digital banking fraud across all platforms in South Africa, 2017–2021

	2017	2018	2019	2020	2021
Incidents	13,389	23,206	26,567	35,307	approx. 29,000
Cost	ZAR251 million	ZAR260 million	ZAR308 million	ZAR310 million	ZAR438 million

Note. Data compiled from SABRIC (2021b) annual crime statistics reports, with financial figures rounded. Where discrepancies arose between reported figures, the most recently reported data was used.

Three of the highest-profile data breaches in South Africa were the hacking of Liberty Life's insurance divisions emails; a breach of the Master Deeds Office, where millions of people's personal information was made available on a public server; and a leak where personal information, including names and identity numbers, was disclosed on the ViewFines website (Adams et al., 2021). During the COVID-19 pandemic, banks identified a trend in scams that took advantage of fear and confusion. These scams sought to (and did) obtain personal information and PIN numbers though compromised business emails and phishing attacks, prompting users to install malware (SABRIC, 2020). Indeed, Van der Merwe's (2020) tally finds that cybercrime in South Africa increased 10-fold in the early period of COVID, a period marked by the announcement of state disaster management actions. Following a synthetic survey of the rise of cyber-incidents in the same period, Van Niekerk et al. (2023) conclude that "while South Africa enacted new legislation to address cybercrime, and the Protection of Personal Information Act became enforceable in 2021, these moves have not come soon enough to mitigate the apparent surge of cybercrime during the pandemic" (2023, p. 199).

In 2021 the banking industry began to openly criticise state capacity in forensic analysis of cybercrimes, a task that the industry believed was urgent given rapid technological changes in consumer products and services:

> Policing plans and the response to cybercrime State Security and policing came under severe scrutiny and criticism due to the breakdown in the effectiveness of these two arms of the state [the police and the National Prosecuting Authority (NPA)]. *The limited capacity of the police and NPA to prevent, detect, investigate, and prosecute cybersecurity breaches, cybercrime, and data breaches is of particular concern.*" (SABRIC, 2021a, p. 8, emphasis added)

Compounding the perceived crisis was a concern that the State Security Agency was more focused on "internal personal and political battles than with assessing and countering external and terrorist threats" (Sutherland, 2017). This lack of credible technical authority leaves citizens unable to assess the veracity of statements from Kaspersky, an antivirus software firm, which has stated that in 2021–22, "over a million company user accounts were compromised using a 'data stealer' in South Africa" (Burbidge, 2022).

Cybersecurity also touches upon identity theft. South Africa has had a complicated history of state-issued identification: During the apartheid era, biometrics were used for state-led surveillance activities aimed at tracking racialised groups (Adams et al., 2021; Breckenridge, 2014). Reports from Parliament's Portfolio Committee on Home Affairs (2013) discuss identity theft and operations at the Government Printing Works. In 2014, the then-Minister of Telecommunications and Postal Services, Siyabonga Cwele, acknowledged that "identity theft has proven to be a very concerning recent phenomenon" (Cwele, 2014). Certainly, a lack of state-issued identification can cause difficulties, and while there are advantages to digital systems, a Research ICT Africa study has found that "digitisation can also introduce novel harms" (Razzano, 2021, p. 4). In July 2013, the government began to issue Smart ID cards while phasing out paper-based documentation (Government of South Africa, n.d.). When examining the draft of the Official Identity Management Policy (Department of Home Affairs, 2020), Research ICT Africa concluded that it was unlikely that existing legislation like the Protection of Personal Information Act, No. 4 of 2013 (POPIA) would be fully implemented (Razzano, 2021).

A report from the Auditor-General of South Africa (2022), under the Public Finance Management Act of 1999, found increases in "irregular expenditure", while there is a "lack of action of potential fraud and corruption and the continued disregard for our findings and recommendations" (2022, p. 61). These weaknesses in governance and accountability have knock-on effects for cybersecurity efforts. The Auditor-General is quick to link the general environment of non-compliance with procurement legislation with "the vulnerability of government systems to cybersecurity attacks because of weak information technology governance and security controls" (2022, p. 62). In 2020–21, the year of the Transnet cyber-incident, the Auditor-General's report identified irregular expenditure of R136.67 billion. This figure could be higher, as some auditees did not follow proper reporting practices with their financial statements. With respect to cybersecurity and the status of information security controls in 2019–20, of the 203 auditees, which included SOEs such as Transnet, 22% were marked as intervention required, 57% marked as concerning, and 21% marked as good (Auditor-General of South Africa, 2022).

The Auditor-General's 2022 report found that the auditees had not made progress towards the objectives outlined in the National Cybersecurity Policy Framework (discussed in the next section), in part because "there were no implementation timelines" (2022, p. 65). The result is that government departments, municipalities, and SOEs "had no choice but to use the State Information Technology Agency's unsupported and vulnerable infrastructure to access their financial systems, which exposed the government to cyberthreats" (2022, p. 65). The Auditor-General has cause to be concerned. The increased reliance on computerised systems for everyday functioning of public and private infrastructure increases the likelihood of attacks, which cause additional economic strain in a country grappling with unemployment, inequality, and poverty.

South African policy and legal framework on cybersecurity

South Africa's regulatory response to cyber-incidents has been slow. One reason may be that the country's criminal common law has traditionally focused on crimes of a tangible nature, especially physical crimes such as murder and theft. Still, the growing threat of cyber-incidents in South Africa has necessitated a response from legislators. Indeed, within Africa, South Africa is subjected to the most attacks and theft by cybercriminals, and this necessitates legal recourse for potential misuse of personal data being accumulated by the public and private sectors, particularly from a human rights perspective (Sutherland, 2017).

One early response to cyber-threats came in the form of the Electronic Communications and Transactions Act, No. 25 of 2002 (ECTA) (Ntsaluba, 2018; RSA, 2002a). Amongst other things, ECTA was enacted to facilitate and regulate electronic communications and transactions in South Africa, provide for the development of a national e-strategy, and encourage the use of e-government services. Furthermore, ECTA mandated provision of universal access to electronic services, i.e., universal access, service, and provision of such services for all communities in South Africa (Adams et al., 2021). ECTA also framed acts that would constitute cybercrimes, including:

- unauthorised access to, interception of, or interference with data;
- computer-related extortion, fraud, and forgery; and
- the aiding and abetting thereof (ECTA, sect. 86–89).

ECTA scoped out a role for cyber inspectors, who have the authority to monitor and inspect websites and web activity in the public domain, as well as to enter premises for search and seizure of information systems on the issuance of a warrant. However, the implementing regulations envisaged by ECTA relating to cyber inspectors and cyber offences were never promulgated, and no cyber inspectors were ever appointed or cyber offences prosecuted under the Act (Sutherland, 2017). As a result, prior to the more recent legislation discussed below, the Consumer Protection Act, No. 68 of 2008 and the common law had to be relied on for the search and seizure of electronic evidence (Govender, 2018).

The Regulation of Interception of Communications and Provision of Communications-Related Information Act, No. 70 of 2002 (RICA), has elements which cover cybersecurity matters and is the key legislation relating to surveillance in South Africa (Adams et al., 2021). The law sought to criminalise acts that may utilise electronic communications including high treason, sedition, fraud, and money laundering (Ntsaluba, 2018). RICA also gave law enforcement entities the power to apply for an interception and monitoring direction, warrants of entry, and made it a criminal offence for any person, without permission, to monitor or intercept any data communications in the public and private sectors (Ntsaluba, 2018). However, despite the intentions of RICA, in the 2021 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* case, certain provisions of RICA relating to surveillance were deemed unconstitutional, leaving the state in a difficult position regarding the rectification of the Act (Global Freedom of Expression, n.d.).

Criminalising certain activities relating to the ICT sector is one facet that comprises the legal framework on cybersecurity in South Africa. Another key area is the protection of the right to privacy. The right to privacy is protected by the 1996 Constitution and provides that every person has the right not to have their person or home searched, their property searched, their possessions seized, or the privacy of their communications infringed. In July 2020, POPIA came into force. POPIA reinforces a person's right to privacy through detailing minimum standards for the accessing and processing of personal information belonging to someone else (Western Cape Government, 2020).

POPIA also ensures that businesses process, share, and store information in a responsible and secure manner, including providing for minimum standards in the event of data breaches (Botha, 2021). POPIA does this by obliging private and public sector organisations to have certain operational and technical security measures in place that protect the privacy of individuals when their personal information is processed (Adams et al., 2021). This may be a useful addition to cybersecurity measures in the country, but may also only be a response to the international political economy with limited enforcement of its provisions. For example, POPIA establishes the office of the Information Regulator, whose responsibilities include monitoring and enforcement of compliance with the Act by both public and private bodies.

In December 2015, the Minister of State Security published the National Cybersecurity Policy Framework (NCPF) for South Africa, although it had been approved by Parliament in 2012. The NCPF was a response to the outcomes-based Justice, Crime Prevention and Security Delivery Agreement, which had as an output that “All People in South Africa Are and Feel Safe” and had the implementation of a Cybersecurity Policy as one of its interventions against cyber-threats of a personal, national, and international nature (Minister of State Security, 2015, p. 75). The NCPF recognised the crucial role that ICTs play in the borderless nature of cybercrimes. Meeting these challenges necessitated adequate security measures as well as a sufficient number of appropriately skilled technicians and engineers, who are in turn correctly tasked (Sutherland, 2017).

The NCPF appraises the vulnerabilities of South Africa’s critical information infrastructure and conceives of a system of preventative measures to protect this infrastructure, and South Africa, against cyber-incidents. The NCPF also seeks to raise public awareness of cybersecurity matters. Furthermore, the NCPF lists measures to address national security from a cyberspace perspective: measures to combat cyber warfare, cybercrime, and other cyber issues; further development of existing laws and ensuring alignment thereof; and measures to ensure confidence and trust in the possibility of ICTs (Minister of State Security, 2015). Despite positive aspirations, doubts have been raised about the government’s ability to adapt and implement the framework, which draws heavily on foreign experiences and texts that may not be applicable to the local context (Sutherland, 2017). The NCPF regards ICTs as indispensable to the functioning of South Africa. Without secure and trustworthy ICT systems, neither the state nor the private sector will function. Countering cyber-threats is therefore essential to the functioning of the economy, and to socioeconomic development.

The Cybercrimes and Cybersecurity Bill (Cyber Bill) followed the NCPF, and was first published for comment in 2015. The final version was released in 2017 (Minister of Justice and Correctional Services, 2017). The Cyber Bill extended the scope of cyber-related crimes beyond those previously provided for in ECTA, and it criminalised additional activities relating to computer systems including, significantly, criminalisation of harmful messages (*BusinessTech*, 2021). The Cyber Bill was challenged on the grounds that, inter alia, its emphasis on the surveillance powers of the state potentially criminalised certain internet freedoms necessary to the work of journalists (Adams et al., 2021). The Cyber Bill was a precursor to the Cybercrimes Act, No. 19 of 2020, which aims to raise South Africa to international standards as far as fighting cybercrime is concerned (Allen, 2021b). However, although the Cyber Bill included provisions on critical information infrastructure and proposed cybersecurity structures, these were not incorporated into the Cybercrimes Act. The Act does, however, include provisions that represent advancements over the content of the Bill, including a clearer definition of cybercrime, criminalisation of unlawful accessing of a computer or device, and prohibition of the following: illegal interception of data; possession, receipt, or use of a stolen password; forgery, fraud, and extortion online; and malicious communications (e.g., via social media) (Allen, 2021b). The Cybercrimes Act also provides authorities with clear guidelines on conducting investigations and collecting cyber evidence—an issue with this is whether the South African Police Service is capable of implementing the Cybercrimes Act due to knowledge and supply constraints (Allen, 2021b).

Finally, there are a number of international and national ancillary and supporting statutes and partnerships that complete the picture of the South African cybersecurity legal framework by addressing issues such as cyberterrorism and cyberwarfare. These include the Protection of Constitutional Democracy against Terrorism Act, No. 33 of 2004; the National Strategic Intelligence Act, No. 39 of 1994; the Critical Infrastructure Protection Bill, 2017; and South Africa's support of the (now defunct) International Multilateral Partnership Against Cyber-Terrorism (Sutherland, 2017). South Africa has also supported a number of resolutions of the UN General Assembly relating to Computer Security Incident Response Teams (CSIRTs), as well as resolutions of the UN Office on Drugs and Crime (Sutherland, 2017). As this section highlights, the legislative framework does not limit cybersecurity to national security, but rather cuts across different sectors. ECTA, for example, is often used as a consumer protection mechanism in the governance of digital transactions.

South Africa is a signatory to the Budapest Convention on Cybercrime (Council of Europe, 2001), but, like Ireland, has not ratified it. This is unsurprising, since the Budapest Convention does not protect human rights and was created in a forum in which South Africa has no voting rights (Rens, 2023). South Africa also signed the African Union Convention on Cyber Security and Personal Data Protection (also known as the Malabo Convention), which, although adopted in June 2014, only received enough ratifications to come into force in May 2023 (AU, 2014). South Africa, like the vast majority of African states, has still not ratified the Malabo Convention. While section 231(1) of the South African Constitution vests the power to negotiate and sign international agreements in the national executive, only Parliament may make international agreements binding in terms of section 231(2). Therefore, signature but non-ratification is the outcome of the constitutional separation of powers and parliamentary reticence (RSA, 1996). As a result, neither Malabo nor Budapest binds South Africa. The provisions of both Budapest and Malabo have become somewhat dated, so a "Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" is currently being negotiated under the auspices of the United Nations, with South Africa as an active participant. The primary benefit of such treaties is to resolve issues of jurisdiction and to facilitate the sharing of evidence across borders.

Criticisms of current legislative and treaty measures include that they are reactive, and implementation remains a problem, making the detection and successful prosecution of cybercriminals onerous. The measures can only be effective to the extent that the state agencies are capable and that attackers are located in South Africa. When attackers are located outside of South Africa, jurisdictional issues immediately complicate investigation and prosecution processes. Although there is growing international cooperation on enforcing laws against cybercrime, given the current state of technology, a reactive response by security agencies cannot prevent ongoing harm to South Africa's economy.

4. Case study of the Transnet cyber-incident

Brief history of Transnet

It is difficult to overstate the role of railways and ports in state- and market-formation in Southern Africa, especially in light of the "mineral revolution" in Southern Africa and its dire consequences (Marks & Rathbone, 1982). After the Second World War, SOEs were a key pillar in the apartheid political economy. Between autarky due to international sanctions, their use to form a white Afrikaner middle class, the intentional creation of rent-seeking structures, and clientelism, the South African Railways and Harbours administration (SAR&H) had acquired considerable asset bases and, in turn, formed part of the commanding heights of the South African economy (Terreblanche, 2002).

Restructuring in the 1970s, re-mandating in the 1980s, and renaming in the 1990s led to the formation of Transnet. Caught up on the wave of privatisation in late apartheid during which the state sought to stave off growing public debt and otherwise maintain an economy already on life support (Reddy & Moodley, 1993), Transnet became corporatised as a SEO. Other notable apartheid restructurings in this period were Telkom and Eskom in 1988, with Iscor following suit in 1989. Trade unions like the South African Municipal Workers Union began organised opposition against corporatisation and joined with the United Democratic Front to make this issue a labour plank within the anti-apartheid movement, helping to fuel strike action and mass mobilisation against the apartheid state. Currently Transnet's board reports to the Minister of Public Enterprises, which functions as its accounting authority and is the shareholder minister with overall executive authority. The company is responsible for the national ports authority, port terminals, freight rail, bulk fuel, and gas pipelines.

Transnet's IT systems

In 2009 Transnet's Risk Management Committee started to examine "technological risks" (Transnet, 2009a, p. 70) as part of the overall efforts aimed at "reengineering its logistics network" (Transnet, 2009b, p. 34) to improve operations and customer service. The following year the company decided to invest ZAR1.9 billion over five years for IT software and licences, including new computers for locomotives and an identification system for wagons (Transnet, 2010). From November 2010, the Chief Information Officer was invited to the board's Risk Committee and Audit Committee meetings. These steps were intended to enhance operational efficiencies while also safeguarding assets. In 2011 planning began to formalise the IT governance structure. The aspiration was to promote sound commercial risk management with IT systems through compliance, appropriate expenditure, and protection of information (Transnet, 2011).

Coinciding with investment, the company began to adopt new IT policies while conducting annual systematic risk assessments. Transnet identified deficiencies like "[i]nadequate ICT infrastructure and technological utilisation to enable the business" (Transnet, 2012, p. 46). The proposed solution to these errors was skills development in the labour force and employing skilled management (Transnet, 2012). Commencing in 2017, Transnet began to deploy an IT architecture that sought to overcome operational silos by moving to group-wide integration (Transnet, 2017, p. 16). Continuing this trend of integrated and shared computer systems, in the following year the Transnet 4.0 Strategy was adopted. This strategy involved the digitalisation of internal and external business processes. The accumulation of other technological refinements—including purchasing and deploying mobile technology in trucks to find route efficiencies—added to operation improvements, Transnet claimed (Transnet, 2018, p. 7).

Annual reports also gave some indication that the company was aware of the potential impact of digital products on the horizon, many linked to machine learning and artificial intelligence (AI) (Transnet, 2018, p. 11; 2019, p. 33). The language in these reports shows that Transnet was eager to embrace these kinds of products, seeing them as potential opportunities without many downsides. At the same time, research conducted by Basson (2017) found that, within Transnet, "several ICT services [were] outsourced depending on the Operating Division (OD), including Active Directory (AD); network infrastructure; CCTV maintenance; fibre cable installations; server management, compliance, and monitoring of ICT services; management of IT systems and workstations in some ODs; and emails and exchange" (Basson, 2017, p. 84). Basson found that concerns over lowering costs plus the shortage of skills and relevant expertise were the main drivers of outsourcing. Additionally, the IT network was deemed "a non-core function"; according to Basson's interviewees, "the outsourcing of ICT [was] also seen as a Transnet strategy to build in-house capacity" (2017, p. 84). In Basson's estimation, any benefits gained by outsourcing were offset by risks associated with infrastructure security.

In 2019 Transnet's self-appraisal of the development of the IT system in the preceding years was scathing. The company indicated that the "organisation [was] not ready to embrace disruptive technologies" in part because of "funding constraints" and in part because "current ICT solutions [were] not integrated" while there was "delayed implementation of new technologies" (Transnet, 2019, p. 37). Proposed interventions were the continuation of converging IT systems between different operating divisions and renewing some legacy systems while phasing out others. There was some attention to cybersecurity initiatives: "With the proliferation of technology in this digital era, Transnet ICT has elevated cybersecurity to a top priority and provides feedback to the Board on a regular basis. It further guards against negative publicity and reputational damage resulting from social media risks" (Transnet, 2019, p. 98). Transnet also revealed that it was subject to cyber-incidents: "Incidents such as ransomware outbreak and cloning of the Transnet.net website have occurred during the course of the year, necessitating the strengthening of our incident response process and ICT continuity management" (Transnet, 2019, p. 98).

Critical self-assessment continued in 2020. Transnet committed itself to the notion of "smart ports" through the implementation of an e-commerce platform and data analytics to optimise the flow of cargo (2020, p. 10). But the company indicated that "our technology roadmap for the business requires an overhaul, we have various conflicting technology paths that are not harmonised towards a common purpose, leading to a misalignment in the digital capabilities of our Operating Divisions" (Transnet, 2020, p. 27). The main weaknesses were "ageing ICT infrastructure and technology" and "cybersecurity", with risk mitigation requiring a "disaster recovery programme" and the drafting of a "Cybersecurity Improvement Plan" (Transnet, 2020, p. 57). The larger point is that Transnet was able to recognise that digitalisation impacted the company's operations, the board was adequately informed over the course of several years that disruptive innovation led to the emergence of new security risks, they were aware of the risks of an aging IT system, and they were aware of prior cybersecurity incidents in other sectors.

Timeline of the Transnet cyber-incident

On 22 July 2021, press reports indicated issues with Transnet's IT network, leading to many logistical operations being conducted manually (e.g., Moyo, 2021). Over the following days, further information revealed that the primary impact was on the movement of cargo at port container terminals. Industry professionals suspected a cyber-incident (Ginindza, 2021), which Transnet confirmed a few days later as they worked to restore IT systems (Khanyile, 2021). A week after the cyber-incident, Transnet declared *force majeure* across all its container terminals due to its inability to meet contractual commitments (Toyana, 2021). Subsequent assessments showed that Durban Port, which handles over half of South Africa's trade, was operating at 10% capacity, resulting in truck turnaround times exceeding 14 hours (Booth, 2021).

From Transnet's self-disclosure, the cyber-incident was a ransomware incident on an IT network. The attacker affected multiple machines before an incident team could securely rebuild the servers using the Microsoft E5 advanced security software package. Endpoint detection and response tools were used to conduct a forensic analysis of the IT system, operating systems were upgraded and patched, and firewalls and other systems were deployed on all public websites before the IT system was brought back online (Transnet 2021c, p. 38). In the interim, transactions were manually recorded, then digitally recorded when the system came online. "As the cybersecurity threat was successfully isolated and contained, none of Transnet's raw data was compromised, affirming that the integrity of all financial and operational information has been maintained," Transnet reported (2021b, p. 127). The Minister of Public Enterprises, Pravin Gordhan, said in mid-August 2021 that Transnet did not pay the ransomware attackers, and that "about 90% of the IT systems at the corporate centre, freight, rail, port terminals, engineering, pipelines, and the port authority, which is slightly behind, are now fully recovered, and the appropriate security measures have been taken" (Gordhan, quoted by Labuschagne, 2021).

Subsequent actions

From its 2021 annual reporting, Transnet reiterated that all aspects of its freight business relied upon ICT, with any failure here creating the risk of the enterprise failing to fulfil its objectives. Transnet's ICT systems are foundational for all areas of the South African economy. With subsequent modification of the IT and Digital Governance committee, there is some indication that Transnet's board recognises its critical role as it took steps to address known IT weaknesses. For example, the board wanted feedback on the organisation's "cybersecurity posture and plans" and indicated that cybersecurity was a "top priority". The same section notes "social media risks", with Transnet needing to protect "against negative publicity and reputational damage" (Transnet, 2021c, p. 32). Additional essential products were purchased to aid its cybersecurity needs (Transnet, 2021c, p. 38).

Other proposed steps included delegating authority to managers to implement IT system management, with the board's Risk Management committee focusing on oversight and implementation of "business continuity arrangement[s]" that allow Transnet to weather any future IT system instability (Transnet, 2021c, p. 38). Another notable change is that cybersecurity acquisitions, incident management, and remedial actions would be undertaken by the ICT Service Management team, which in turn reports to the Enterprise Technology Services functional unit (Transnet, 2021c, p. 39). Transnet indicated that all of these actions would adhere to existing laws, including POPIA.

Finally, Transnet reaffirmed its commitment "to employ a digital-first culture to digitise both existing and next-generation products and services". The company has shown interest in computational products that could drive digital transformation, and is eager to leverage "disruptive and enabling technologies" through strategic partnerships for "agile and innovative services (Transnet, 2021c, p. 39). This presents some cause for concern, as in past years Transnet has been overly influenced by Silicon Valley marketing hype, often at the expense of managing its more routine IT systems. While AI could potentially yield efficiency gains in the future, at present it has demonstrated increased cybersecurity risks.

5. Analysis and discussion

Over the past decade, Transnet's board has exhibited corporate governance practices that have failed to meet the operational needs of its IT systems. Annual reports reveal the board's awareness of years of underinvestment in IT architecture and cybersecurity, a result of economic mismanagement and budget constraints that hindered the overhaul of vulnerable legacy systems. The company recognised and attempted to address the fragmentation in its IT enterprise system, but the efforts were belated. In a corporate entity like Transnet, such fragmentation hinders the realisation of economies of scale, reducing global competitiveness (Timmers, 2018).

Additionally, the board has lacked the foresight to recognise how cybersecurity breaches occurring elsewhere in the world in similar enterprises might also happen to its organisation. The main risk is that shipping lines could shift their export capacity and use their fleets on other trade routes, which would have cascading effects across the South African economy. There is also little indication of industry cooperation and pooling of expertise. Transnet's reporting makes claims that known deficiencies in the IT system have been addressed; however, to date there has been no public third-party verification of this exercise. Transnet did seem to recognise that cyber incidents erode trust, and that even one incident factors into other entities' risk management assessments.

An additional concern is the apparent lack of urgency from the South African state in enforcing cybersecurity procedures. Despite having the legal authority to direct Transnet to adopt benchmark cybersecurity products, this oversight seems to indicate a failure to recognise that the line between physical and digital critical infrastructure is increasingly blurring. This significant conceptual oversight is evident in the Department of Public Enterprises' 2021/2022 annual report (DPE, 2022), which does not adequately address the cyber-incident against Transnet or highlight it as a potential warning for other SOEs.

In conclusion, we find that both the board of Transnet and the Department of Public Enterprises demonstrated a lack of practical understanding of IT systems. Furthermore, there was a deficit in imagination in both entities, as they failed to fully acknowledge the increasing prevalence of cyber-incidents worldwide and did not foresee that such attacks could impact them. The lack of evidence that, at present, the South African state acknowledges either the risks of weak cybersecurity, or the added complexities introduced by AI, suggests that the national economy remains highly vulnerable to cyber-incidents. Conversely, without coherence, coordination, trust, and understanding, the prospects of establishing an effective developmental state are diminished.

6. Conclusion

As the strong dependency of the South African economy on Transnet illustrates, cybersecurity in SOEs is a matter for socioeconomic development policy. Without the purchase and system-wide installation of benchmarked cybersecurity products, when security compromises occur they negatively impact the South African government's endeavours towards actualisation of the developmental state in the domestic market, as well as support for trade with land-locked countries in the region. Another key consideration is how cyber-incidents have a negative impact on the monetary inflows on which South Africa depends. There are valid questions around whether the corporatisation of SOEs leads to underinvestment in cybersecurity, as returns to shareholders take priority over secure IT systems. Therefore, there may be merit in the government relaxing the imperative to return value to the shareholder—itself—and instead to insist on due investment to upgrade computational hardware and software systems. Transnet is just one example of an SOE that, if compromised due to inadequate cybersecurity, could severely damage the South African economy and exacerbate the burdens on the poor and powerless.

There is value in cultivating a deeper appreciation for the necessity for advanced cybersecurity protection in South African SOEs. The efficiency and effectiveness of SOEs, and consequently the delivery of state services, and the provision of infrastructure on which markets depend are significantly influenced by cybersecurity. Without a secure bulk freight network, municipal trading services may struggle to source and acquire components for their water, sanitation, electricity, safety, and access infrastructure, for example. Similar considerations apply to a secure electrical supply. The inescapable conclusion is that cybersecurity is a cornerstone of an effective democratic developmental state.

References

Adams, R., Pienaar, G., Olorunju, N., Gaffley, M., Gastrow, M., Thipanyane, T., ... Adams, F. (2021). *Human rights and the fourth industrial revolution in South Africa*. HSRC Press. https://doi.org/10.1515/9780796926173

African National Congress (ANC). (1994). The Reconstruction and Development Programme (RDP). https://www.sahistory.org.za/sites/default/files/the_reconstruction_and_development_programm_1994.pdf

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

Allen, K. (2021a, March 9). Critical infrastructure attacks: Why South Africa should worry. *ISS Today*. Institute for Security Studies. https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry

Allen, K. (2021b, June 9). South Africa lays down the law on cybercrime: Despite major implementation challenges, the new legislation signals the country's commitment to global cyber security. *ISS Today*. Institute for Security Studies. https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime

*AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Service*s [2021] ZACC 3 (Constitutional Court). https://www.saflii.org/za/cases/ZACC/2021/3.html

Auditor-General of South Africa. (2022). *PFMA 2021–22: Consolidated general report on national and provincial audit outcomes.* https://www.agsa.co.za/Reporting/PFMAReports/PFMA2021-22.aspx

Basson, D. J. (2017). *Managing infrastructure risks in information communication technology outsourced projects: A case study at Transnet, South Africa* [Master's dissertation]. Cape Peninsula University of Technology, Cape Town.

BBC. (2019, July 26). Ransomware hits Johannesburg electricity supply. *BBC.* https://www.bbc.com/news/technology-49125853

Beach, D. (2017). Process tracing in the social sciences. In *Oxford research encyclopedia of politics*. https://doi.org/10.1093/acrefore/9780190228637.013.176

Booth, I. (2021, July 28). Transnet cyberattack could have catastrophic consequences. *Investec Focus*. https://www.investec.com/en_za/focus/economy/transnet-cyberattack-could-have-catastrophic-consequences.html

Botha, R. (2021, June 8). Understanding POPI and its impact on cybersecurity. *Media Update*. https://mediaupdate.co.za/marketing/150645/understanding-popi-and-its-impact-on-cybersecurity

Breckenridge, K. (2014). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to present*. Cambridge University Press. https://doi.org/10.1017/CBO9781139939546

Burbidge, M. (2022, November 28). Over a million user accounts "stolen" in South Africa. *ITWeb*. https://www.itweb.co.za/content/GxwQD71Da5ZvlPVo

BusinessTech. (2021, December 2). South Africa's new cybercrime laws have been partially introduced – here's what comes next. https://businesstech.co.za/news/technology/543432/south-africas-new-cybercrime-laws-have-been-partially-introduced-heres-what-comes-next/

Chang, H. J. (2007). *State-owned enterprise reform*. UN Department of Economic and Social Affairs (UN DESA) Policy Notes. https://edisciplinas.usp.br/pluginfile.php/154675/mod_resource/content/1/ic-chang.pdf

Collier, D. (2011). Understanding process tracing. *PS: Political Science & Politics*, *44*(4), 823–830. https://doi.org/10.1017/S1049096511001429

Council of Europe. (2001). Budapest Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/home

Crees, S. (2020). *Artificial intelligence and the law.* Routledge.

Cwele, S. (2014). Minister of Telecommunications and Postal Services budget speech. Briefing, 16 July. Parliamentary Monitoring Group. https://pmg.org.za/briefing/19078/

Department of Finance. (1996). Growth, Employment and Redistribution: A Macroeconomic Strategy. https://www.treasury.gov.za/publications/other/gear/chapters.pdf

Department of Home Affairs. (2020). Draft Official Identity Management Policy (public consultation version). http://www.dha.gov.za/images/PDFs/Draft_Official_Identity_Management_Policy_-_Gazette_Version_of_22122020.pdf

Department of Public Enterprises (DPE). (2000). An Accelerated Agenda towards the Restructuring of State Owned Enterprises: Policy Framework. https://www.gov.za/sites/default/files/gcis_document/201409/acceleratedagendarestructuringsoe0.pdf

DPE. (2022). *Annual report 2021/2022*. https://dpe.gov.za/wp-content/uploads/2022/09/DPE-AR2022-d13.pdf

Erwin, A. (2004). Public Enterprises Dept Budget Vote 2004/2005, Ministry of Public Enterprises, 14 June. Parliamentary Monitoring Group. https://static.pmg.org.za/docs/2004/appendices/040609erwin.htm

European Investment Bank. (2022). *European cybersecurity investment platform*. https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf

Evans, P. (1995). *Embedded autonomy: States and industrial transformation*. Princeton University Press. https://doi.org/10.1515/9781400821723

Fourie, D. (2022). The neoliberal influence on South Africa's early democracy and its shortfalls in addressing economic inequality. *Philosophy & Social Criticism*. https://doi.org/10.1177/01914537221079674

Gall, G. (1997). Trade unions and the ANC in the "new" South Africa. *Review of African Political Economy*, *24*(72), 203–218. https://doi.org/10.1080/03056249708704253

Ginindza, B. (2021, July 23). Transnet "cyber attack" causes logistics logjam from road to freight and ports. *IOL*. https://www.iol.co.za/business-report/economy/transnet-cyber-attack-causes-logistics-logjam-from-road-to-freight-and-ports-56f6bd97-c5ef-4d65-90d6-c41d0fe290e2

Global Freedom of Expression. (n.d.). *Amabhungane Centre for Investigative Journalism v. Minister of Justice and Correctional Services*. https://globalfreedomofexpression.columbia.edu/cases/amabhungane-centre-for-investigative-journalism-v-minister-of-justice-and-correctional-services/

Govender, T. F. (2018). *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* [LLM dissertation]. University of KwaZulu-Natal, Durban.

Government of South Africa. (n.d.). Smart identity document (ID) card roll-out. https://www.gov.za/about-government/government-programmes/smart-identity-document-id-card-roll-out

Gumede, W. (2009). *Delivering the democratic developmental state in South Africa*. Development Planning Division Working Paper Series No. 9. Development Bank of Southern Africa (DBSA).

Gumede, W. (2016). The political economy of state-owned enterprises restructuring in South Africa. *Journal of Governance & Public Policy*, *6*(2), 69–97.

Hogan, B. (2009). Public Enterprises: Minister's budget speech, 22 June. Parliamentary Monitoring Group. https://pmg.org.za/briefing/18715/

Institute of Directors in Southern Africa (IoDSA), & King Committee on Corporate Governance. (2016). *Report on corporate governance for South Africa 2016 (King IV)*. https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf

Interpol. (2021). *African cyberthreat assessment report*. https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

Johnson, C. (1982). *MITI and the Japanese miracle: The growth of industrial policy, 1925–1975*. Stanford University Press. https://doi.org/10.1515/9780804765602

Khanyile, G. (2021, July 27). Significant progress made in restoring Transnet IT systems. *IOL*. https://www.iol.co.za/dailynews/news/significant-progress-made-in-restoring-transnet-it-systems-2b83efff-31e1-4378-92d6-6c30c336c539

Labuschagne, H. (2021, August 17). Transnet ransomware hackers did not get a single cent. *MyBroadband*. https://mybroadband.co.za/news/security/410058-transnet-ransomware-hackers-did-not-get-a-single-cent.html

Leftwich, A. (1996). On the primacy of politics in development. In A. Leftwich (Ed.), *Democracy and development: Theory and practice*. Polity Press.

Marks, S., & Rathbone, R. (Eds.). (1982). *Industrialisation and social change in South Africa: African class formation, culture, and consciousness, 1870–1930*. Longman.

Mayedwa, V. A. (2018). *The role of the state-owned enterprises in the developmental state of South Africa: A case study of Transnet*. http://vital.seals.ac.za:8080/vital/access/manager/Repository/vital:32028?site_name=GlobalView

Mazzucato, M. (2013). *The entrepreneurial state: Debunking public vs. private sector myths*. Anthem Press.

Minister of Justice and Correctional Services. (2017). Cybercrimes and Cybersecurity Bill, 21 February. https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6-2017-21-feb-2017-0000

Minister of State Security. (2015). The National Cybersecurity Policy Framework, 4 December. https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

Moyo, A. (2021, July 22). Transnet suffers "disruption" of IT systems. *ITWeb*. https://www.itweb.co.za/content/wbrpOqgYAwY7DLZn

Muller, S. M., Amra, R., & Jantjies, D. (2015). Report on State-Owned Enterprises. Parliamentary Standing Committee on Finance. https://static.pmg.org.za/150812report.pdf

Ntsaluba, N. (2018). *Cybersecurity policy and legislation in South Africa* [Master's dissertation]. University of Pretoria.

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication (AJIC)*, *28*, 1–21. https://doi.org/10.23962/10539/32213

Portfolio Committee on Home Affairs. (2013). ATC130503: Report of the Portfolio Committee on Home Affairs on the Annual Performance Plan and Budget Vote 4 of the Department of Home Affairs and its entities, 30 April. Parliamentary Monitoring Group. https://pmg.org.za/tabled-committee-report/1396/

Qian, Y., & Sun, Y. (2021). The correlation between annual reports' narratives and business performance: A retrospective analysis. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211032198

Razzano, G. (2021). *Digital identity in South Africa: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT Africa (RIA). https://researchictafrica.net/publication/digital-identity-in-south-africa-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa

Reddy, P. S., & Moodley, D. (1993). Privatisation of public corporations in South Africa: The issue re-examined. *Africanus*, *23*(1). https://hdl.handle.net/10520/AJA0304615X_262

Rens, A. (2023, August 29). The negotiations for a global cybercrime convention, global public goods and AI cyber risk [Blog post]. Research ICT Africa (RIA). https://researchictafrica.net/2023/08/29/the-negotiations-for-a-global-cybercrime-convention-global-public-goods-and-ai-cyberisk/

Republic of South Africa (RSA). (1996). Constitution of the Republic of South Africa Act, No. 108 of 1996.

RSA. (2002a). Electronic Communications and Transactions Act, No. 25 of 2002 (ECTA).

RSA. (2002b). Regulation of Interception of Communications and Provision of Communications-Related Information Act, No. 70 of 2002 (RICA).

RSA. (2013). Protection of Personal Information Act, No. 4 of 2013 (POPIA).

RSA. (2020). Cybercrimes Act, No. 19 of 2020.

South African Banking Risk Information Centre (SABRIC). (2012). *Card fraud South Africa, 2011–2012*. https://www.sabric.co.za/media/c2ljwaww/2011-to-2012-card-fraud-booklet.pdf

SABRIC. (2017). *Card fraud booklet 2017*. https://www.sabric.co.za/media/tjigbdjl/2017-card-fraud-booklet.pdf

SABRIC. (2020). *Annual report 2020*. https://www.sabric.co.za/media/lejmweri/sabric_annual-report_2020.pdf

SABRIC. (2021a). *Annual report 2021*. https://www.sabric.co.za/media/z0vch20l/sabric-annual-report-2021.pdf

SABRIC. (2021b). *Annual crime statistics 2021*. https://www.sabric.co.za/media/5dlnhnyj/sabric-crime-stats-2021_fa.pdf

Sen, A. (1999). *Development as freedom*. Oxford University Press.

Shaw, M. (2018, January 9). Known unknowns: The threat of cybercrime in Africa. *ISS Today*. Institute for Security Studies. https://issafrica.org/iss-today/known-unknowns-the-threat-of-cybercrime-in-africa

Southall, R. (2013). Realism and neoliberalism: Macro-economic policy in South Africa. In J. Curry (Ed.), *Liberation movements in power: Party and state in Southern Africa* (pp. 88–96). University of KwaZulu-Natal Press.

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

Terreblanche, S. (2002). *A history of inequality in South Africa, 1652–2002*. University of KwaZulu-Natal Press.

The Presidency. (2011). National Development Plan 2030: Our Future – Make it Work (Executive summary). National Planning Commission. Government of the Republic of South Africa.

The Presidency. (2012). *Report of the Presidential Review Committee on State-owned Entities: Volume 1: Executive summary of the final report*. Government of South Africa. https://www.gov.za/sites/default/files/gcis_document/201409/presreview.pdf

The Presidency. (2019, September 27). President appoints Economic Advisory Council [Press release]. https://www.thepresidency.gov.za/press-statements/president-appoints-economic-advisory-council

Thomas, A. (2000). Poverty and the “end of development”. In T. Allen & A. Thomas (Eds.), *Poverty and development into the 21st century*. Oxford University Press.

Tijerina, W. (2022). Industrial policy and governments’ cybersecurity capacity: A tale of two developments? *Journal of Cyber Policy*, 7(2), 194–212. https://doi.org/10.1080/23738871.2022.2071747

Timcke, S. (2017). *Capital, state, empire: The new American way of digital warfare*. University of Westminster Press. https://doi.org/10.16997/book6

Timcke, S. (2023). *The political economy of fortune and misfortune*. Bristol University Press. https://doi.org/10.1332/policypress/9781529221756.001.0001

Timcke, S., & Gaffley, M. (2022, December 8). RIA’s public comment on National Infrastructure Plan 2050. Research ICT Africa. https://researchictafrica.net/2023/01/05/ria-public-comment-national-infrastructure-plan-2050/

Timcke, S., Gaffley, M., & Rens, A. (2023). *A single point of failure: Transnet's IT network and the risk of AI-cybersecurity gaps to the South African developmental state project*. Working Paper, Research ICT Africa (RIA).

Timmers, P. (2018). The European Union's cybersecurity industrial policy. *Journal of Cyber Policy*, *3*(3), 363–384. https://doi.org/10.1080/23738871.2018.1562560

Toyana, M. (2021, July 27). Transnet ports division declares force majeure on container terminals after cyber attack. *Daily Maverick*. https://www.dailymaverick.co.za/article/2021-07-27-transnet-ports-division-declares-force-majeure-on-container-terminals-after-cyber-attack/

Transnet. (2009a). *Limited annual report 2009, corporate governance*. https://www.transnet.net/InvestorRelations/AR/2009/Corporate%20Governance.pdf

Transnet. (2009b). *Limited annual report 2009, executive summary*. https://www.transnet.net/InvestorRelations/AR/2009/Executive%20%20Summaries.pdf

Transnet. (2010). *Annual results 2010, operational report*. https://www.transnet.net/InvestorRelations/AR/2010/Operational%20Reports.pdf

Transnet. (2011). *Quantum leap, integrated annual report 2011*. https://www.transnet.net/InvestorRelations/AR/2011/Integrated%20Report.pdf

Transnet. (2012). *Integrated report 2012*. https://www.transnet.net/InvestorRelations/AR/2012/Integrated%20Report.pdf

Transnet. (2013). *Integrated report 2013*. https://www.transnet.net/InvestorRelations/AR/2013/Integrated%20Report.pdf

Transnet. (2014). *Integrated report 2014*. https://www.transnet.net/InvestorRelations/AR/2014/Integrated%20Report.pdf.

Transnet. (2015). *Integrated report 2015*. https://www.transnet.net/InvestorRelations/AR2015/2015/downloads/Transnet_IR_2015_190715.pdf

Transnet. (2016). *Integrated report 2016*. https://www.transnet.net/InvestorRelations/AR2016/2016/downloads/TRANSNET-IR-2016.pdf.

Transnet. (2017). *Integrated report 2017*. https://www.transnet.net/InvestorRelations/AR2017/Transnet%20IR%202017.pdf

Transnet. (2018). *Integrated report 2018*. https://www.transnet.net/InvestorRelations/AR2018/Transnet%20IR%202018.pdf

Transnet. (2019). *Integrated report 2019*. https://www.transnet.net/InvestorRelations/AR2019/Transnet%20IR%202019.pdf

Transnet. (2020). *Integrated report 2020*. https://www.transnet.net/InvestorRelations/AR2020/Transnet%20IR%202020.pdf

Transnet. (2021a). *Repair and grow: Annual results announcement*. https://www.transnet.net/InvestorRelations/AR2021/2021%20ANNUAL%20RESULTS%20PRESENTATION.pdf

Transnet. (2021b). *Integrated report 2021*. https://www.transnet.net/InvestorRelations/AR2021/Transnet%20Integrated%20Report.pdf

Transnet. (2021c). *Transnet governance report 2021*. https://www.transnet.net/InvestorRelations/AR2021/Governance%20report%2028%20Oct.pdf

Transnet. (2022). *Unabridged governance report 2022*. https://www.transnet.net/InvestorRelations/AR2022/Governance%20report%202022.pdf

Ukwandu, D. C. (2019). South Africa as a developmental state: Is it a viable idea? *African Journal of Public Affairs*, *11*(2), 41–62.

United Nations Conference on Trade and Development (UNCTAD). (2007). *Economic development in Africa: Reclaiming policy space: Domestic resource mobilisation and developmental states.* https://unctad.org/system/files/official-document/aldcafrica2007_en.pdf

Van der Merwe, P. (2020, March 26). Unprecedented spike in cyber attacks since declaration of national disaster. *TimesLive*. https://www.timeslive.co.za/news/south-africa/2020-03-26-unprecedented-spike-in-cyber-attacks-since-declaration-of-national-disaster/

Van Heerden, R., Von Soms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa, 2016. In *2016 IST-Africa Week Conference* (pp. 1–16). https://doi.org/10.1109/ISTAFRICA.2016.7530663

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Van Niekerk, B., Ramluckan, T., & Collard, A. (2023). A South African perspective on cybercrime during the pandemic. In D. Ventre & H. Loiseau (Eds.), *Cybercrime during the SARS-CoV-2 pandemic (2019-2022): Evolutions, adaptations, consequences* (pp. 177–209). ISTE and Wiley. https://doi.org/10.1002/9781394226344.ch6

Venter, I. (2022, March 31). White Paper on rail lauded as SA loses at least 1% of GDP to Transnet inefficiency. *Creamer Media's Engineering News*. https://www.engineeringnews.co.za/article/white-paper-on-rail-lauded-as-country-loses-1-of-gdp-to-transnet-inefficiency-2022-03-31

Western Cape Government. (2020, October 6). An introduction to the Protection of Personal Information Act (or POPI Act or POPIA). https://www.westerncape.gov.za/site-page/introduction-protection-personal-information-act-or-popi-act-or-popia.

World Bank. (2008). New directions in development thinking. In G. Secondi (Ed.), *The development economics reader.* Routledge.