A Single Point of Failure

Transnet's IT network and the risk of AI-cybersecurity gaps to the South African developmental state project

Scott Timcke and Mark Gaffley with Andrew Rens

April 2023

Working Paper

RESEARCH ICT AFRICA

Workshop17
17 Dock Road
V&A Waterfront
8001
Phone: +27 21 447 6332
www.researchictafrica.net

About Research ICT Africa

Research ICT Africa (RIA) is an African think tank that has operated for over a decade to fill a strategic gap in the development of a sustainable information society and digital economy. It has done so by building the multidisciplinary research capacity needed to inform evidence-based policy and effective regulation in Africa. RIA's dynamic and evolving research agenda examines the uneven distribution of the benefits and harms of the intensifying global processes of digitalisation and datafication.

On this basis, RIA seeks to provide alternative policy and regulatory strategies that produce different outcomes that will address digital inequality in Africa and enable data justice. Through rigorous research and analysis RIA seeks to build an African knowledge base in support of digital equality and data justice, and to monitor and review developments on the continent.

About Just AI

The research informing this submission was made possible by a three-year grant from Canada's International Development Research Centre (IDRC) and the Swedish International Development Cooperation Agency (SIDA) as part of RIA's Africa Just AI Project (Just AI Project), an AI Policy Research Centre that aims to ensure AI development and decision-making are carried out in accordance with ethical systems and a rights-respecting framework. The authors are currently engaged in public interest research as part of the project under the AI Risk and Cybersecurity theme.

More broadly, the Just AI Project relies on knowledge grounded in the historical and contemporary contexts of African countries, advocating for people-centred, beneficial AI innovation, and building local capacity and awareness, both for the development of AI systems and their just governance. In this way, the Just AI Project brings international and continental human rights instruments into national policy and regulation, moving away from AI ethics discourses driven by multinationals, as well as researchers and activists from the Global North. More information on the project can be found here.

Acknowledgements

Thanks are due to Andrew Rens and Rachel Adams for early influence. Same too with Enrico Calandro and Thuli Olorunju who provided helpful reviews. Charmaine Smith's cheerful editorial support was much appreciated.

Table of Contents

1 Executive summary

This policy paper forms part of the broader project to understand what factors amplify or diminish the risks to markets and society in Africa from, by, and with advanced computational systems. To address this and other related "big questions", we use process-tracing methods to examine what factors need to be considered in the formation of an industrial policy calibrated to anticipate and respond to the everyday risks of cybersecurity, artificial intelligence (AI) software included.

We examine relevant legislation and corporate governance decisions in the decade prior to the breach of the South African Transnet information technology (IT) network in July 2021 to support this broader policy analysis. This case provides an opportunity to derive insights about what sorts of measures the Government of South Africa can consider adopting in the near future if it wishes to safeguard the digital, administrative and mechanical systems that are vital for circulation of commodities.

Another reason we focus on the Transnet cyberattack is because it is a high profile event in a critical sector where catastrophic failure would near guarantee cascading consequences that would strain South African society, as well as nearby landlocked countries that rely upon this bulk freight complex. This case attests to the industrial implications of cybersecurity as well as the wider impact of cybersecurity on state–society dynamics.

Our overarching argument is that cybersecurity can no longer be thought of as the sole province of the state security cluster. As the Transnet cyber-attack well illustrates, cybersecurity policy is industrial policy. Viewed from this perspective, a developmental state must have a central role in creating trusted marketplaces, not only in terms of the legal and policy space, but also in procurement of suitable security software systems for the various state-owned enterprises that shoulder the economy.

As state-owned enterprises are prominent in the South African economy – and will be for the foreseeable future – it is crucial that there is an examination of how their performance with AI and cybersecurity technologies can be improved. What matters is how cybersecurity is linked to the state's efforts to address the triple-fold challenges of unemployment, inequality and poverty.

South Africa has a developed, if uneven, infrastructure with a relatively high degree of digitisation although there is insufficient government capacity to ward against cyber threats. With AI technologies becoming more accessible to the everyday person the world over, failure to act constitutes a major threat to the smooth functioning of the South African market and the people that rely on that economy.

Attaining a sufficient level of cybersecurity is a desirable priority. While the case study focuses on a single state-owned enterprise in South Africa, the implications are much wider. While South Africa has more advanced infrastructure than many other African countries, the case study provides an important experience that other countries should draw on as they develop logistics, other infrastructure, and begin introducing cybersecurity measures.

2 Introduction

Transnet is a state-owned enterprise in South Africa. The company is responsible for ports, rail, and pipelines and is a monopoly in bulk freight. In 2000 Transnet directly contributed 3.2% to the national GDP (Department of Public Enterprises, 2000, p. 137), with a greater indirect contribution as all exports happen, or not, subject to the efficiency of Transnet. This is why recent capacity problems mean that export earnings in the mining and agriculture sectors are lower than what they could be, up to R50 billion (±US$2.79 billion, see Venter, 2022). Although state monopolies have structural pros and cons depending on their purposes and conditions, when these entities supply critical services including electricity, telecommunications, port and rail infrastructure they present a single point of vulnerability to cyber-attacks.[1] For present purposes, a cyber-attack is an attempt to damage a computer network and/or IT system.

Building upon a highly visible ransomware attack on Johannesburg's electricity supply in 2019 (BBC, 2019), South African analysts sought to raise awareness to government, key stakeholders, and citizens about the vulnerability of critical infrastructure. Efforts intensified in early 2021 (e.g. Allen, 2021a). A few months later, in July 2021, the Transnet cyber-attack occurred with IT systems being unavailable for use at cargo terminals. This disruption added to global supply chain problems caused by the coronavirus pandemic. The public was notified of the incident by the press, with Transnet issuing statements over the next few days. The company was not very forthcoming about details at the time. More remarks were provided in various subsequent public annual reporting documents 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" (Transne,t 2021a, p. 25).

As we argue throughout this paper, both AI and cybersecurity are core matters for a country's industrial 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 Walid Tijerina (2022, p. 194). This deficit must be remedied if one views cybersecurity in relation to the political economy of risk and the disproportionate burdens that emerge from that political economy. Indeed, harms to avoid can include targeted and accidental threats arising from our daily use such as loss of access to digital services (Creese, 2020). These mundane risks that affect the ordinary citizen bring the question of cybersecurity out of a parochial

[1] There is a dogmatic view that outright rejects government ownership of any sort, claiming that state-owned enterprises (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 supposedly leads to fiscal crises and with the state repeatedly having to bail out these entities. Nevertheless this conclusion does not concede that state-owned enterprises might have other purposes and values than the ones the dogmatists prefer to maximise. Indeed, some state-owned enterprises exist to address market failures or operate in sectors that are unlikely to ever be profitable and hence be adequately served by private firms. In short, state-owned enterprises are political entities and their performance should be evaluated from the vantage point of the interplay between several agendas and competing objectives. Ha-Joon Chang summarises the literature on state-owned enterprises by writing that there "is no clear theoretical case either for or against SOEs" as well as there being "no clear systemic evidence that SOEs are burdens on the economy" (Chang 2007, pp. 7-8).

perspective which treat cybersecurity as exclusively a state security issue. With these research, risk and issue gaps in mind, this paper uses the experience of the July 2021 Transnet cyber-attack to gain a better understanding of how compromised IT systems hinder not only trusted market activity, but also point to governance areas that require reinforcement with policy. As state-owned enterprises are prominent in the South African economy – and will be for the foreseeable future – it is crucial that there is an examination of how their performance with AI and cybersecurity technologies can be improved, and what the implications of risk are and for whom. AI is an important technological development, as are the cyber risks in this area; nevertheless attention must include broader matters that sit in relation to the mandate of the state to address the triple-fold challenges of unemployment, inequality and poverty. All three of which can be exacerbated through the harm cyber poses, including in areas that exist outside of cyberspace (Creese, 2020).

It is beyond the scope of this study to corroborate or negate specific hypotheses about the identities and motivations of the Transnet cyber-attack hackers, especially given the contemporary (as well as contentious) nature of the matter. Rather we discuss how these kinds of matters relate to the South African government's industrial policy towards freight, ports and other networks, as well as the potential social costs given the IT networks in state-owned enterprises are the fulcrum of the South African economy at large, at least in the view that this policy paper advances. Estimates of costs arising from cybersecurity breaches to the South African economy exist, but there is opacity about what activities the calculations included and how tallies were derived. Therefore the figures must be critically viewed as a heuristic.[2] Besides which, past costs are less useful to guide projections about future losses if cyber-attacks target critical infrastructure, especially so when AI-software products are becoming a common part of the attacker's toolkit.

As the July 2021 cyber-attack targeted a state-owned enterprise, by necessity we look to link operational issues with larger governance issues. In South Africa, state-owned enterprises are guided by a developmental state project. While we will cover the history and politics of this project as it relates to AI and cybersecurity, one starting point to understand this project is 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). As United Nations Conference on Trade and Development (UNCTAD) explains, 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" (2007, pp. 59-60), an undertaking Amartya Sen says is "a process of expanding the real freedoms that people enjoy" (1999, p. 36).

Much of what Sen refers to requires achieving economic development. Economic development is a qualitative shift in economic structure and the relationship 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, efficiency and

[2] Figures were circulated of R3.7 billion in direct losses in 2011, R50 billion in 2014 (van Niekerk, 2017), R43 billion in 2016 (Interpol, 2021), R5.7 billion in 2018 (Shaw, 2018). As a point of reference, in 2021 South Africa's GDP was about R7 trillion (±US$420 billion).

competitiveness of downstream industries are directly related to the efficiency and competitiveness of this component of the logistics sector. Therefore the measures that Transnet takes to secure operations around bulk freight and logistics, directly and indirectly impact on 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 future alleviation of poverty and inequality.

2.1 Method and data sources

The main method in this policy paper is process tracing guided by precepts from historical materialism.[3] The method studies how "causal processes work using case study methods" (Beach, 2017). 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). The main data source for process tracing in this paper is the narratives of business performance in annual reports (see 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 editions of the King Commission on Corporate Governance (2016, also see Section 4.3) – there is scope to augment objective audited figures with the written judgements of executives and their management teams.

Narratives in annual reporting show how executives and their management teams conceptualised past and future actions, as well as give some indication of what actions they intend to take to safeguard the financial wellbeing of the business. Certainly "narratives in corporate annual reports are intentionally manipulated by the informant", still overarching fiduciary requirements and auditory compliance do shape these narratives as well; this means "these reports [can] help to uncover current, corporate operating conditions, and reveal future potential from the management point of view rhetorical aspects of voluntary disclosure" (Qian & Sun, 2021, p. 1). In this paper we prioritised the study of Transnet's annual reporting from 2009 to 2022, focusing on the self-assessments of risk in and to its IT systems.

2.2 Organisation

The first half of the paper addresses the politics over the form that the South African state and society would take in the post-apartheid era. It is in this cauldron that industrial policy is formed and decisions about the forms of governance for state-owned enterprises are established. Thereafter the paper discusses AI and cybersecurity matters in South Africa from a legal perspective. Taking inspiration from how existing protection of information legislation foregrounds rights against undue

[3] Historical materialism is a diverse academic methodology that has been applied to a wide variety of political and economic processes. It is beyond the scope of this paper to discuss how historical materialism can be used to analyse cybersecurity; still the analysis of state capitalism and social relations can provide critical insights into the class aspects of cybersecurity.

exploitation, the general point is to show that there are grounds to treat cybersecurity in a broader manner, wider than simply being seen as a national security issue.

Following this groundwork, the second half of the paper presents a case study of the Transnet cyber-attack. Drawing on more than a decade of governance reports, this section traces Transnet's expenditure plans for its IT architecture. After noting some discrepancies between planning and actual investments, we look at what actions the board of Transnet undertook following the cyber-attack. In doing so we use the Transnet cyber-attack as a case study to derive insights about the broader risks cyber presents to South Africa's industrial policy.

Finally, after discussing what wider factors amplify or diminish the risks to markets in South Africa from, by, and with advanced computational systems, and what that means for the prospect of attaining economic justice and human rights, we address what sorts of measures the Government of South Africa can consider adopting if it wishes to safeguard the digital, administrative and mechanical systems that are vital for circulation of commodities in the developmental state model. At the end of the paper we provide some general takeaways for countries facing similar situations, whether in Africa or elsewhere in the majority world.

3 The developmental state model

It is beyond the scope of this paper to comprehensively detail the intense two decade-long politics between the state, capital, and labour (and factions within all three) over the structure and purpose of state-owned enterprises in post-apartheid South Africa. Still, a short contextual description can provide a useful primer on the considerations that lead 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 state-owned enterprises (Presidential Review Committee on State-owned Entities, 2012, p. 67). Many of these enterprises existed due to duplication of function 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 selected privatisation of state-owned enterprises as a means to reduce the state's debt. Additional considerations were the desire to court foreign direct investment by boosting market confidence, thereby signalling a new policy course 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 to eradicate poverty and attain humane, meaningful and sustainable livelihoods (see 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 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 development state can be traced to a few sources including the ANC's 1995 Reconstruction and Development Programme and 1996 Growth, Employment, and Redistribution (GEAR) macroeconomic policies, and can also be extrapolated from the later chapters of the 1996 South African Constitution. The developmental state model was more clearly articulated in the Government of South Africa's successive *Medium-Term Strategic Frameworks*, and planning documents like the *National Development Plan: 2030*.

A developmental state is a government that actively promotes economic development through state intervention in strategic areas such as infrastructure, education, and industrial policy. The strategic priorities and intent of South Africa's developmental state project aims to:

- Speed up growth and transform the economy to create decent work and sustainable livelihoods;
- Undertake a massive programme to build economic and social infrastructure;
- Establish a comprehensive rural development strategy linked to land, agrarian reform and food security;
- Strengthen the skills and human resource base;
- Improve the health profile of all South Africans;
- Intensify the fight against crime and corruption;
- Build cohesive, caring and sustainable communities;
- Pursue African advancement and enhanced international cooperation;
- Advance sustainable resource management and use; and
- Build a developmental state, including improvement of public services and strengthening democratic institutions.

(Slight modification from the Presidential Review Committee on State-owned Entities, 2012, 34-35)

Like other areas of South African society formed during the transition to democratic rule in the 1990s, the developmental state model is a "negotiated compromise between the ANC's long standing embrace of planned development through nationalisation'' (Mandela quoted in *Mail & Guardian,* 1990) 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 (see Southall, 2013; Gumede, 2016; Fourie 2022). More broadly, the model aims to stoke capitalist development through active state-led industrial 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 Chalmers Johnson (1982) and Peter Evans (1995), among others. In recent years the model has been supplemented by Mariana Mazzucato's (2013) research on the entrepreneurial state, which is an updated redescription of the positive core benefits of state intervention into the market. Indeed, President Cyril Ramaphosa appointed Mazzucato to the Presidential Economic Advisory Council in October 2019 (Presidency, 2019), a signal that the developmental state model remains at the forefront of many South African state officials, even if local academics are more circumspect about the state's

performance and structure (e.g., Ukandu, 2019) and the capability of state-owned enterprises to deliver this mandate (e.g., Gumede, 2016).

Turning from models of political economy to policy matters, the adoption of GEAR in 1996 as a macroeconomic strategy sought to provide a policy framework in which state-owned enterprises could become more efficient and provide effective services for the public (see Department of Public Enterprises, 2000). Given that the ANC relied heavily on organised labour movements to attain and maintain rule, massive unions like the Congress of South African Trade Unions (COSATU) felt betrayed by the privatisation agenda (Gall, 1997). After taking strike action, the government and organised labour signed the National Framework Agreement in early 1996 which sets out terms for restructuring on a case-by-case basis over the next three years, taking into account the impact on workers.

Early in his presidency, Thabo Mbeki articulated that:

"GEAR sets out a number of macro principles and targets to which we remain committed. These include: fiscal discipline, achieved through deficit reduction; continued liberalisation of exchange controls; accelerated reduction in tariffs; tax incentives to fund training; accelerated delivery on the backlog of social infrastructure; maintenance of a stable and competitive exchange rate; labour market reform to increase the absorptive capacity of the economy; and the privatisation and restructuring of state assets." (Mbeki, 1999)

Nevertheless, the government proceeded with restructuring state-owned enterprises, 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 state-owned enterprises, a practice that every president of South Africa has earnestly defended despite continuous criticism. Black business groups encouraged privatisation as the use of preferential procurement strategies by state-owned enterprises could create a black capitalist class. By contrast, labour was wary of the consequences of a firesale of state property (Gumede, 2016). Indeed, it was only when Minister of Public Enterprises, Alec Erwin (2004–2008), who was very perceptive to how the pursuit of private profit can clash with the pursuit of the public good, that state-owned enterprises faced these competing considerations (see 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 they had built and maintained. Barbara Hogan, the then Minister of Public Enterprises (2009–2010) sums up the outcome: the "disposal of non-core assets in the Transnet stable has enabled the corporation to focus on its core business" (Hogan, 2009).

4 AI and cybersecurity in the South African context

4.1 General conceptualisation of AI and cybersecurity

The growing use of AI in various computational systems has led to the emergence of new risks, including those associated with cybersecurity. The rapid evolution of AI risks can (and is) changing how organisations protect sensitive information from unauthorised access. Autonomous adversarial attacks may receive the lion's share of attention, but as Matthew Ford and Andrew Hoskins (2022) discuss, dependencies on generic entry-level consumer and corporate IT systems can create a single point of failure which may compromise the overall security of an organisation (also see Rens, Calandro & Gaffley, 2022; Timcke, 2022). These mundane risks are the most vulnerable to advances in software. Even in the non-technical realm, AI can be used to generate impersonated correspondence for a mass phishing exercise; machine learning can also aid with the increased scale and effectiveness of cyber-attacks by manipulating enterprise AI through inputs, causing misinterpretations that favour an attacker.

Adversarial attacks can certainly use AI to scout for weak points. Setting aside state espionage, cybercrime activities can breach IT systems, taking it as a hostage for extortion. This act is known as "ransomware" (see O'Kane, Sezer & Carlin, 2018). It is important for public policy to prioritise understanding the range, extent, and implications of the AI-enabled cybersecurity risk. This includes examining the potential harm that AI deployment can cause to digital networks and systems, societies, organisations, and individuals. This can include issues such as AI-enabled cyber-attacks on critical infrastructure, the use of AI to spread disinformation or influence elections, as well as the use of AI to perpetuate existing social biases or amplify misconceptions. AI systems can also be the target of attacks. It is crucial that state officials and policymakers work with experts in AI and cybersecurity with the intent to understand and comprehensively address these risks in an effective manner.

Beyond the state, there is an entire international political economy of AI-enabled risk that also constitutes the uses and abuses of technology (see Timcke, 2017; Timcke, 2022). What we mean is that transnational economic forces and political objectives influence the development and deployment of AI systems, notwithstanding the potential risks associated with these technologies. These factors include government policies and regulations, corporate investment and competition, and global trade and economic relations.

The international political economy of AI risk also encompasses the social and ethical implications of AI, such as issues related to privacy, autonomy, and the potential for AI to be used for malicious purposes. This political economy shapes the distribution, circulation and exposure to risk, as well as the differences in power and position between those that produce AI systems and those that feel the sharp effects of those systems. In short, AI is often linked to broader issues of social and economic injustice. To elaborate, AI risk can intersect with patterned prejudice like institutional racism. It is most often people within poor, underserved communities that are more likely to be subject to the hazards from AI, for example (Intahchomphoo & Gundersen, 2020) or are more likely to face unequal enforcement of AI regulations while also lacking the capacity to exercise their digital civil rights. Put simply, AI and institutional racism can reinforce systemic discrimination with serious consequences

for affected communities. While those international actors are set to reap many of the benefits of AI systems, the risks are largely borne by others, including the public sector in Africa. Though beyond the scope of this study, it is worth noting blind spots inherent in popular AI ethics discourse around explainability, algorithmic fairness and privacy that may also perpetuate discriminatory practices instead of addressing them (see Hagendorff, 2021). Similarly, there are potential blind spots, oversights and issues relating to impartiality if cybersecurity issues are "owned" by the state security cluster with certain functions it had pertaining to surveillance even being deemed unconstitutional because of its infringement on the right to privacy (Global Freedom of Expression, n.d.).

Lastly, given the enduring impact of colonial underdevelopment in Africa, people living on the continent do not have the same material, institutional, or fiscal resources to mitigate cybersecurity risks as do their former colonial occupiers. A related factor is that post-colonial state re-formation typically occurred under neocolonial fiscal relationships which insisted on structural adjustment programmes where austerity policies staved public institutions of resources. Public administration lost technical skills and institutional knowledge for a generation. This is an abbreviated list of why African countries are not well positioned to address cybersecurity vulnerabilities in general, and why current risk assessment and mitigation frameworks may need to be adjusted to account for more fundamental vulnerabilities that may be taken for granted elsewhere.

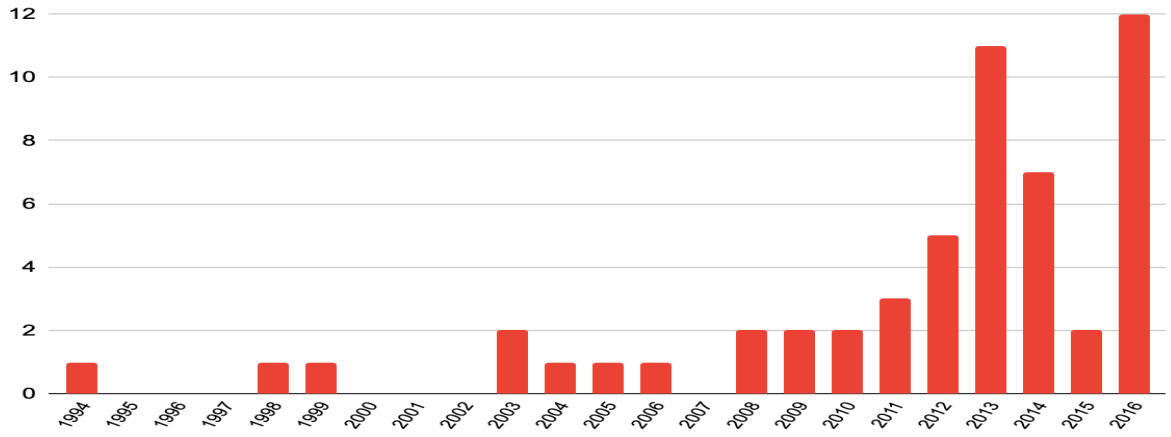
Incident Type	Number
Data Exposure	22
Financial	12
Denial of Service	9
Defacement	8
Data Corruption	2
System Penetration	1

Table 1: Types of documented cyber incidents, 1994–2016 (data from van Niekerk, 2017).

4.2 Known cyber-incidents in South Africa

Between 1994 and 2016, Brett van Niekerk (2017) identified 54 documented cyber incidents (Table 1; see van Heerden et. al., 2016 for classification schema). There were three cyber incidents prior to 2002, but most happened from 2003 onwards, and with more surging in recent 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 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. This research has heuristic merit, but one limitation of van Niekerk's data is that it cannot show severity and does not speak to the scale of these incidents. As an example, 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.

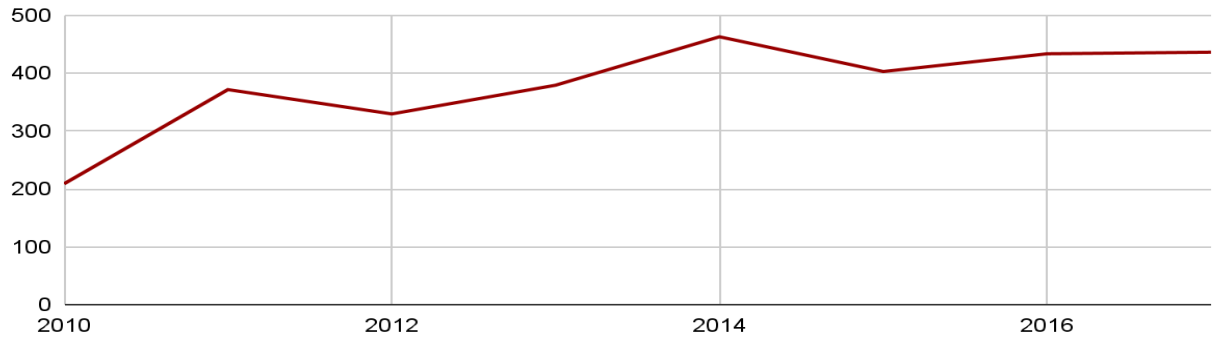
Within the same period of van Niekerk's research, the banking industry experienced a rise in credit card fraud (see Graph 2). This activity prompted banks to put risk-detection and prevention systems by increasing the rollout of chip and pin systems (SABRIC, 2012). During the course of 2018, the South 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"; they add "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 costs of digital crime between 2017 and 2021, with the number of incidents also rising.



Graph 1: Frequency of documented cyber incidents in South Africa (data from van Niekerk, 2017).

Three high-profile data breaches in South Africa include the hacking of Liberty Life's insurance divisions emails; a breach of the Master Deeds Office where millions of peoples' personal information was made available on a public server; and a leak where personal information, including names and identity numbers were disclosed on the ViewFines website (Adams, et. al., 2021). During the coronavirus 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). In 2021, the banking industry began to openly criticise state capacity in cyber forensic analysis in cybercrime, a task the industry believes is 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 limited capacity of the police and NPA to prevent, detect, investigate, and prosecute cybersecurity breaches, cybercrime, and data breaches is of particular concern*" (SABRIC, 2021, p. 8, emphasis added). Compounding this are concerns raised that the State Security Agency is 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 claimed that since

2021 “over a million company user accounts were compromised using a ‘data stealer’ in South Africa” (Burbidge, 2022).



Graph 2: Fraud loss on SA-issued credit cards, 2010–2017 (data from SABRIC, 2017).

Cybersecurity also touches upon identity theft. South Africa has had a long complicated history of state-issued identification during the apartheid era when biometrics were used for state-led surveillance activities aimed at tracking migrant workers and organisational capabilities of computing technologies enforced censorship laws (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 (2014), acknowledged that “identity theft has proven to be a very concerning recent phenomenon.” 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, nd.). 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, 4 of 2013 (POPIA) would be fully implemented (Razzano, 2021).

	2017	2018	2019	2020	2021
Incidents	13,389	23,206	26,567	35,307	±29,000
Cost	R251 million	R260 million	R308 million	R310 million	R438 million

Table 2: Digital banking fraud across all platforms in South Africa, 2017–2021. (Data compiled from SABRIC annual crime statistics reports with financial figures rounded. Where conflicts arise, the more recently reported data was used.)

Finally, reporting from the Auditor-General of South Africa under the Public Finance Management Act of 1999 has repeatedly 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" (Auditor-General of South Africa 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 attack, irregular expenditure was R136.67 billion. This figure could be higher as some auditees did not follow proper reporting practices with their financial statements. When looking at cybersecurity and the status of information security controls in 2019-20, of the 203 auditees, which included state-owned enterprises like Transnet, 22% were marked as intervention required, 57% marked as concerning, and 21% marked as good. The Auditor-General assesses that the auditees have 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 state-owned enterprises "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 cybertreats" (2022, p. 65).

4.3 The South African legal framework on cybersecurity

As discussed, responses to cyber-attacks can include technical measures to control access to networks and devices, to detect compromise of networks, and to restore data and systems that have been damaged. However these measures have not proven efficacious on their own, so authorities have sought to criminalise cyber-attacks to deter them as well as to implement minimum standards for organisations to adhere to. While merely rearranging data may not appear to be criminal harm, it can lead to physical harm and damage or economic loss. That is often the intent. Increased reliance on computerised systems for everyday functioning of public and private infrastructure increases the likelihood of attacks which disrupt economic activity.

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

One initial response to cyber threats came in the form of the Electronic Communications and Transactions Act, 25 of 2002 (ECTA) (Ntsaluba, 2018). 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 to encourage the use of e-government services.

Furthermore, ECTA committed to providing universal access to electronic services, which includes universal access, service and provision of such services for all communities in South Africa (Adams et. al., 2021). Seen in this light, cyber's imperative as a tool of industrial policy is emphasised. 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 (see ECTA, ss86-69).

ECTA also 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 enter premises for search and seizure of information systems on the issuance of a warrant. However, 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 ECTA (Sutherland, 2017). As a consequence, prior to more recent legislation discussed below, the Consumer Protection Act, 68 of 2008 and common law had to be relied on for search and seizure of electronic evidence (Govender, 2018).

The Regulation of Interception of Communications and Provision of Communications-Related Information Act, 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 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Correctional Services and Others*, 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 right to privacy, which can be dated as far back to the 1950s in the country, when a photograph was published in an advert without the consent of the person in the image (Sutherland, 2017; O'Keeffe v Argus Printing, 1954). The right to privacy is now 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 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 public and private bodies (see section 40), yet there is no information available which indicates Transnet reported to the Information Regulator following its security breach or whether any investigation or penalties were issued by the office of the Information Regulator.

In December 2015, the Minister of State Security published the National CyberSecurity Policy Framework for South Africa. 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 (NCPF, 2015). The NCPF recognised the crucial role ICT technologies 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 provides a strategy that appraises vulnerabilities of South Africa's critical infrastructure and conceives of a system of preventative measures against cyber-attacks and attempts to raise public awareness. Furthermore, the NCPF lists measures to address national security from a cyberspace perspective; measures to combat cyber warfare, cybercrime and other cyber issues; the development of existing laws and ensuring the alignment thereof; as well as measures to ensure confidence and trust in the possibility of ICT technologies (NCPF, 2015). Despite positive aspirations, criticism has been raised against the Government of South Africa concerning its 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 Cybercrime and Cybersecurity Bill (Cyber Bill) followed the NCPF and was first published for comments in 2015 and with the final version being released in 2017 (Ntsaluba, 2018). The Cyber Bill extended the scope of cyber-related crimes not previously provided for in ECTA and criminalised more activities relating to computer systems. A key advancement was the criminalisation of harmful messages (BusinessTech, 2021). The Cyber Bill was, however, challenged on the basis that it potentially criminalised certain journalistic internet freedoms because of its emphasis on surveillance powers of the state (Adams et al., 2021). The Cyber Bill also acted as a precursor to the Cybercrimes Act, 19 of 2020 (Cybercrimes Act) which aims to raise South Africa to international standards as far as fighting cybercrime is concerned (Allen, 2021b). Advancements include providing a more clear definition of cybercrime, criminalising unlawful accessing of a computer or device, prohibiting illegal interception of data, possession, receipt or use of a password and forgery, fraud and extortion online, as well as malicious communications (e.g., via social media) (Allen, 2021). 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 Services is capable of implementing the Cybercrimes Act due to knowledge and supply constraints (Allen, 2021).

Finally, there are a number of international and national ancillary and supporting legislation 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, 33 of 2004; National Strategic Intelligence Act, 39 of 1994; 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 CSIRTS, as well as the UN Office on Drugs and Crime (Sutherland, 2017). This said, as this section highlights, the legislative framework does not limit cybersecurity to national security, but cuts across different sectors. The ECTA, for example, is often used as a consumer protection mechanism in the governance of digital transactions.

The biggest criticisms of current legislative measures include the fact 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 the 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.

5 Case study of the Transnet cyber-attack

5.1 Brief history of Transnet

It is difficult to overstate the role of railways and ports in state- and market-formation in Southern Africa. Following the success of railways during European industrialization, the technology was imported by the British to the Cape to aid with resource extraction of agriculture from the southwest of Cape Town to world markets. A secondary objective was to better settle the Karoo. The Cape Town Railway and Dock Company was formed in 1853 with a 16% shareholding by the Cape Colony Government. Rail construction began the next year albeit with limited operations (Goodfellow, 2023). Other regions in the Cape Colony likewise sought railways lines to serve the ports of East London and Port Elizabeth, but geography and commodity type (in this case wool) made raising finance difficult. A local depression throughout the 1860s compounded these arduous conditions.

The discovery of a diamond field in Kimberly in 1869 and then a gold reef in the Witwatersrand in 1884 changed the fiscal calculations for investment in rail infrastructure to support exports of these resources. Once built, whether as strategic assets for the British to move troops during the Second Boer War (1899–1902) or to bring (black) migrant labour to mines, railways and ports were key components in the "mineral revolution" in Southern Africa and its dire consequences (Marks & Rathbone, 1982). With the establishment of the Union of South Africa in 1910, the transport systems of the four provinces were amalgamated to form the South African Railways and Harbours Administration (SAR&H). In 1930, Union Airways (now South African Airways) would become an arm of the SAR&H, although it would later be detached. After the Second World War, state-owned enterprises

were a key pillar in the apartheid political economy. Between autarky due to international sanctions, their use to form and consolidate a white Afrikaner middle class, the intentional creation of rent seeking structures, and clientelism, entities such as SAR&H had acquired considerable asset bases and, in turn, forming part of the commanding heights of the South African economy (see Terreblanche, 2002).

More recently, restructuring in the 1970s, remandating 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 re-regulate in an attempt to stave off growing public debt and otherwise maintain a political economy already on life support (see Reddy & Moodley, 1993), Transnet became corporatised as a state-owned enterprise. Other notable apartheid restructurings in this period were Telkom and Eskom in 1988 and 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. To provide a sense of Transnet's strategic importance to trade flows in the South African economy, in 2021 (the year of the Transnet cyber-attack) nine commodities made up ±43% of the GDP, and contributed 80% of Transnet's revenue. The company has a property portfolio of R35 billion (±US$2 billion) which includes industrial warehousing, commercial, retail, and residential property. Lockdowns during the global coronavirus pandemic greatly impacted Transnet's revenue, which in 2021 was down 10.5% to R67.3 billion (±US$3.94 billion) with a R8.7 billion loss (±US$500 million). In 2022, revenue increased by 1.8% to R68.5 billion with a net profit of R5.0 billion, mostly coming from a 5.9% decrease in operating expenses via voluntary severance packages (Transnet, 2021a).

5.2 Recent history of 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 R1.9 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 Risk Committee and Board 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 that deficiencies in IT systems had the highest consequence, judging that there was a greater than 50% chance of an incident occurring. Internal vulnerabilities were attributed to "inadequate ICT infrastructure and poor technology utilisation" which would result in "human error, reduced productivity and financial loss". 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. 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. The aspiration was unmoored from reality.

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 AI. 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 Delton Basson (2017) found that "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-attacks, "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 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" (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, they were aware of the risks of an ageing IT system, and they were aware of prior cybersecurity attacks.

5.3 Timeline of the Transnet cyber-attack

On July 22, 2021 there were initial press reports that there was a problem with Transnet's IT network with many logistical operations being done manually (e.g., Moyo, 2021). Over the coming days drips of information revealed the extent of the problem with the movement of cargo at port container terminals primarily affected. Industry professionals believed it was a cyber-attack (Ginindza, 2021), with Transnet confirming the case a few days later while restoring IT systems (Khanyile, 2021). Transnet declared itself unable to meet contractual commitments due to *force majeure* across all its container terminals a week after the cyber-attack (Toyana, 2021). From subsequent assessment, the Durban Port – which deals with more than half of South Africa's trade – was only able to operate at 10% capacity; trucks experienced upwards of a 14-hour turn-around time (Booth, 2021).

From Transnet's self disclosure, the cyber-attack 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, firewalls and other systems were deployed on all public websites before the IT system was brought back online (see 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 at the time, Pravin Gordhan, said in mid-August 2021 that Transnet did not pay the ransomers, 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).

5.4 Subsequent actions

From its 2021 annual reporting, Transnet reiterated that all aspects of their freight business relied upon ICT, with any failure here creating the risk of the enterprise from fulfilling its objectives. In not too many words, 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" (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". As in the years before, Transnet stressed its interest in much hyped computational products that may shape a digital transformation. Transnet is keen to embrace "disruptive and enabling technologies" by "leveraging an ecosystem that includes strategic partnerships to ensure that ICT provides agile and innovative services" (Transnet, 2021c, p. 39). This presents some cause for concern, as in years past Transnet gave too much credence to the marketing hype emanating from Silicon Valley, letting the necessity of day-to-day management of more ordinary IT systems recede from attention.

6 Analysis and discussion of social costs

Over the past decade Transnet's board demonstrated reckless corporate governance practices which did not align with the day-to-day needs of the IT systems it had in place. From a review of self-disclosed evidence in annual reporting documents, it is clear that the Transnet board was aware of the company's years of underinvestment in IT architecture and cybersecurity. These are among the long-term consequences of economic mismanagement and budgetary constraints leading to the inability to overhaul vulnerable legacy systems. It is clear that fragmentation in the IT enterprise system was a problem Transnet was aware of and sought to address, but too late. With a corporate entity like Transnet, fragmentation prevents taking advantage of economies of scale, meaning that the enterprise is less globally competitive (see Timmers, 2018).

Additionally the Transnet board lacked the foresight to recognise how cybersecurity breaches occurring elsewhere in the world in similar enterprises might also happen to their organisation. The main risk is that shipping lines could shift their export capacity and utilise 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 does also seem to recognise that cyber incidents erode trust, and that one incident is a broad signal to the world that other entities will use it as an example when conducting their own risk management exercises.

Another area of concern is how generally unconcerned owners (i.e. the South African state) were with insisting on cybersecurity procedures. As owners, the South African government has the legal basis to instruct Transnet and other state-owned enterprises to purchase benchmark cybersecurity products. Seemingly, from this oversight one can conclude that there is a lack of comprehension that there is no longer any meaningful distinction between physical and digital critical infrastructure. This major conceptual failure is evident in the Department of Public Enterprises 2021/2022 annual report (DPE, 2022) where the cyber-attack against Transnet is not meaningfully covered. Nor does the report flag the incident as a warning signal for potential deficiencies in other state-owned enterprises. In short, there is very little indication from the South African state that it has realised the risks of weak cybersecurity, let alone how particular styles of AI software might further complicate the operating environment. Without vision and leadership by the South African state to insist that the boards of its various state-owned enterprises address cybersecurity issues, the risks to the national economy remain incredibly high. Conversely, the chance of creating an effective developmental state remains low without coherence, coordination, completement, trust, and understanding.

Ultimately, we find that the board of Transnet and the Government of South Africa, as the owner of this state-owned enterprise, lacked a pragmatic understanding of IT systems. At the same time we find an imaginative deficit in both entities, insofar as neither fully appreciated how cyber-attacks were becoming commonplace throughout the world; the board and the state could not imagine that these kinds of attacks could affect them.

6.1 Cybersecurity is a matter for industrial policy

As the near dependency of the South African economy on Transnet well illustrates, cybersecurity in state-owned enterprises is a matter for industrial policy. Without the purchase and system-wide installation of benchmarked cybersecurity products, when security compromises do occur they negatively impact the Government of South Africa's endeavours to actualise the developmental state in the domestic market, as well as support trade for other land-locked countries in the region. Another key consideration is how cyber-attacks like these have a negative impact on monetary inflows on which South Africa depends. There are valid questions around whether the corporatisation of state-owned enterprises leads to underinvestment in cybersecurity as returns to shareholders take priority over secure IT systems. As such, there may be merit in the Government of South Africa relaxing the imperative to return value to shareholders and instead to insist on due investment to upgrade computational hardware and software systems.

Transnet is only one example of a state-owned enterprise that, if compromised due to insufficient cybersecurity, will severely damage the economy and amplify the already too heavy burdens on the

poor and powerless. Presently, South Africa is hampered by an electrical power supply crisis. The social costs of a cyber-attack that damages or destroys the IT architecture of Eskom would be considerable. Furthermore, as there is much discussion about the South African state licensing private electricity generation while larger municipalities envision selling electricity to the national grid, any smart grid system will need to be resilient to cyber-attacks. The integration of supply from multiple suppliers to multiple customers will have multiple control systems and databases that will necessarily be accessible through the Internet (see National Smart Grid Vision for the South African Electricity Supply Industry, 2022). A smart grid is highly likely to be targeted. A smart grid in India has been subject to attack (Sanger & Schmall, 2021).

A further consideration is that attackers may not only use system weaknesses to exploit vulnerabilities, but also for commodification of unrelated ventures, particularly as far as private and sensitive data is concerned (Adams et al,, 2021). Indeed, precedent exists in South Africa where social grant recipients were taken advantage of by the payment service providers entrusted with the digitisation of state grant payments (Gaffley, 2021), revealing that cyber risks do not lie solely with criminal elements. It is likely that these kinds of systems, which are increasingly likely to rely on AI, would be thoroughly tested by cyber-attackers using AI technologies to support their probes for weaknesses. A smart grid will integrate state-owned enterprises together with national, provincial and municipal government entities and private providers and users. All of these have to co-operate to ensure that the smart grid is secured from cyber-attacks. This requires setting common standards for all the participants and independent assessment and coordination mechanisms to prevent, respond to and recover from attacks.

The moment is ripe for a re-conceptualisation of the role, need, and value of advanced cybersecurity protection in major state-owned enterprises like Transnet. Cybersecurity informs the efficiency and effectiveness of state-owned enterprises with respect to subsequent state service delivery. Indeed the provision of basic public services, especially for the poor and powerless, rests on this realisation. Without a bulk freight network it is difficult for municipal trading services, for example, to source and acquire components for their water, sanitation, electricity, safety and access infrastructure. Similar considerations attach to a secure electrical supply. The inescapable conclusion is that cybersecurity is a cornerstone component of an effective developmental state.

7 Recommendations for promoting cybersecurity within industrial policy

Immediate actions can help guide the formation of an integrated long-term development plan to reinforce the cybersecurity component of industrial policy in the political economy of a developmental state. Our major recommendations for the Government of South Africa are to:

- Develop a common understanding of the cybersecurity realm for SOEs which stresses the importance of cybersecurity within the developmental state paradigm. This could be accomplished through additions to existing Government plans, like the National Infrastructure Plan 2050 Phase 2 presently with the Department of Public Works and Infrastructure;

- Attain a better understanding of the strategic importance of cybersecurity, and how cybersecurity can protect the value chains that hinge on SOEs like Transnet;
- Identify strategic sectors and critical infrastructure which can benefit from cybersecurity and accordingly prioritise investment to procure suitable enterprise quality cybersecurity software packages;
- Understand how the existing portfolio of investments by the state in strategic businesses can be protected by cybersecurity, thereby optimising the use of state resources;
- Add to existing standardised accounting and reporting processes for SOEs that address practical cybersecurity matters, which in turn can help maintain trusted marketplaces;
- Recruit, select and appoint boards and executive management of SOEs where some members have technical cybersecurity experience. To reinforce a previous point, there is value for state officials and policymakers to work with experts in AI and cybersecurity so that they can better comprehend and address risks in these areas;
- Improve the relationship and collaboration between national, provincial and local government departments to facilitate achievement of cybersecurity objectives which will also go a long way towards restoring perceptions of government credibility;
- Invest in a domestic cybersecurity industry. Initial steps would include a market gap analysis, the financial landscape for source of funds, and the larger technological ecosystem;
- Recognising that cybersecurity is a matter of industrial policy, ensure cybersecurity and related cyber risk assessments and measures are not shrouded in unnecessary or counterproductive secrecy by government (Sutherland, 2017);
- Commission research by a third party to assess cybersecurity readiness within state-owned enterprises. This research could in turn recommend staffing hiring profiles and additional executive competencies;
- Create sector-specific mechanisms to set cybersecurity standards, conduct independent reviews, provide oversight, and convene cybersecurity co-operative teams; and
- Develop sufficient capacity to undertake monitoring and evaluation exercises, thereby reducing the need for outside consultants from the private or non-profit sectors.

Depending on circumstance and context, some of these general recommendations may be useful for countries and governments facing similar sets of considerations, whether in Africa or elsewhere in the majority world.

8 About the authors

Scott Timcke (PhD, Simon Fraser) is a political economist whose primary area of expertise is in democratic development policy, industrialisation, and the role of the state in promoting egalitarian social and economic development. He leads the Information Disorders and AI Risk and Cybersecurity projects at RIA. He can be contacted at stimcke@researchictafrica.net.

Mark Gaffley is an admitted attorney with over 10 years of start-up, in-house legal and research experience gained through leading local and international companies and think tanks including Uber, Takealot, Media24, Human Sciences Research Council, and Research ICT Africa. He worked at RIA as a Researcher and Project Manager: AI, and has also run his own legal consultancy for the past three years. He can be contacted at mgaffley@researchictafrica.net.

9 Bibliography

Adams, R. et al. (2021). *Human Rights and the Fourth Industrial Revolution in South Africa.* HSRC Press.

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

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

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* [Unpublished M-Tech dissertation] Cape Peninsula University of Technology.

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

Beach, D. (2022). Process tracing in the social sciences. *Oxford Research Encyclopedia of Politics*, 25 January. https://doi.org/10.1093/acrefore/9780190228637.013.176.

Booth, I. (2021, July 28). *Transnet cyberattack could have catastrophic consequences*. Investec, 28 July 2021.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.

Burbidge, M. (2022, November 28). Over a million user accounts 'stolen' in South Africa. *IT Web*. 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. *BusinessTech.* 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, policy notes. United Nations, Department of Economic and Social Affairs*.
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. doi:10.1017/S1049096511001429

Crees, S. (2020). The threat from AI. In *Artificial Intelligence and the Law.* Routledge.

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. (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*. Department of Public Enterprises. https://dpe.gov.za/wp-content/uploads/2022/09/DPE-AR2022-d13.pdf

Electronic Communications and Transactions Act, No. 25 of 2002.

Erwin, A. (2004). Public Enterprises Dept Budget Vote 2004/2005, Ministry of Public Enterprises, 14 June 2004. *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.

Ford, M., & Hoskins., A. (2022). *Radical war: Data, attention and control in the 21st century.* Hurst.

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

Gaffley, M. (2021). *AI and data in South Africa's finance sector: Toward financial inclusion*. Policy Action Network.
https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData9_FinServices_V1_Elec.pdf

Gall, G. (1997). Trade unions & the ANC in the “new” South Africa. *Review of African Political Economy, 24*(72), pp. 203-218. http://www.jstor.org/stable/4006430

Ginindza, B. (2021, 23 July). 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/

Goodfellow, D. M. (2023 [1931]). *An economic history of South Africa*. Routledge.

Govender, T. (2018). A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa [Unpublished Master’s degree thesis]. University of KwaZulu-Natal. https://ukzn-dspace.ukzn.ac.za/bitstream/handle/10413/16567/Govender_Terrina_2018.pdf?sequence%E2%80%89=%E2%80%891%26isAllowed%E2%80%89=%E2%80%89y

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.

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

Hagendorff, T. (2021). Blind spots in AI ethics. *AI and Ethics, 2*(2022), pp. 851–867.

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

Intahchomphoo, C., & Gundersen, O. (2020). Artificial intelligence and race: A systematic review. *Legal Information Management, 20*(2), pp. 74-84. doi:10.1017/S1472669620000183

Interpol. (2021). *African cyberthreat assessment.* 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.

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-31e1-4378-92d6-6c30c336c539King Commission on Corporate Governance & Institute of Directors in South Africa. . (2016). *Report on corporate governance for South Africa 2016*. https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf

Labuschagne, H. (2021, August 17). Transnet ransomware hackers did not get a single cent. *My Broadband.* 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.

Mail & Guardian. (1990, 26 January). Mail we will nationalise — Mandela. *Mail & Guardian*., https://mg.co.za/article/1990-01-26-we-will-nationalise-mandela/

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

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

Mbeki, T. (1999). A*ddress by President Thabo Mbeki at the SA-USA Business and Finance Forum, Roosevelt Hotel, New York, 23 September 1999.* South Africa History Online, https://www.sahistory.org.za/archive/address-president-thabo-mbeki-sa-usa-business-and-finance-forum-roosevelt-hotel-new-york-23

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

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

Ntsaluba, N. (2018). Cybersecurity policy and legislation in South Africa [Unpublished master's degree thesis]. University of Pretoria. https://repository.up.ac.za/bitstream/handle/2263/65706/Ntsaluba_Secutiry_2018.pdf?sequence=1&isAllowed=y.

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks, 7*(5), pp. 321-327. https://doi.org/10.1049/iet-net.2017.0207

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 2013.* Parliamentary Monitoring Group. https://pmg.org.za/tabled-committee-report/1396/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. (2019, September 2017). *President appoints Economic Advisory Council [Press release].* https://www.thepresidency.gov.za/press-statements/president-appoints-economic-advisory-council.

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

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 (Towards the Evaluation of Digital ID Ecosystems in Africa: Findings from Ten Countries)* [Case study]. Research ICT Africa . 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

Regulation of Interception of Communications and Provision of Communications-Related Information Act, No. 70 of 2002.

Rens, A. Calandro, E. & Gaffley, M. (2022, March 22). As global cyber conflict breaks out, AI technologies bring new risk to Africa. *RIA Blog.* https://researchictafrica.net/2022/03/23/as-global-cyber-conflict-breaks-out-ai-technologies-bring-new-risk-to-africa/

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

SABRIC. (2020). *Annual report 2020*. South African Banking Risk Information Centre. https://www.sabric.co.za/media/lejmweri/sabric_annual-report_2020.pdf

SABRIC. (2021). *Annual crime statistics 2021*. South African Banking Risk Information Centre https://www.sabric.co.za/media/5dlnhnyj/sabric-crime-stats-2021_fa.pdf.

SABRIC. (2021). *Annual report 2021*. South African Banking Risk Information Centre., https://www.sabric.co.za/media/z0vch20l/sabric-annual-report-2021.pdf

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

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

Southall R. (2013). Realism and neoliberalism: Marco-economic policy in South Africa. In J. Curry (Ed.). *Liberation movements in power: Party & 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*, *20*, pp. 83-112. DOI: 10.23962/10539/23574

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

Thomas, A. (2000). Poverty and the 'end of development'. In T. Allen, T., & 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), pp. 194-212. DOI: 10.1080/23738871.2022.2071747

Timcke, S. (2017). *Capital, state, empire: The new American way of digital warfare*. University of Westminster Press.

Timcke, S. (2022, July 18). Book review: Radical war: Data, attention and control in the twenty-first century by Matthew Ford and Andrew Hoskins. *LSE Review of Books.*, https://blogs.lse.ac.uk/lsereviewofbooks/2022/07/18/book-review-radical-war-data-attention-and-control-in-the-twenty-first-century-by-matthew-ford-and-andrew-hoskins/

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/

Timmers, P. (2018). The European Union's cybersecurity industrial policy. *Journal of Cyber Policy, 3*(3), pp. 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. (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

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

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

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

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

Venter, I. (2022, 31 March). 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

World Bank. (2008). New directions in development thinking. In G. Secondi (Ed.). *The Development Economics Reader.* Routledge.