

P O L I C Y B R I E F

DR. FAITH TINONETSANA

JUNE 2025



Addressing the Rise of Cyberattacks in South Africa

Executive summary

Globally, developments in science, telecommunications, automation, and artificial intelligence have been rapid. The widespread access to these advancements has meant that most societies rely on technological tools for a range of services. However, this has resulted in challenges emerging within the cybersecurity landscape. South Africa has not been immune to such challenges and measures must be implemented to address the increasing cyber threats and risks in order to reduce the vulnerability of society and the economy (including businesses).

These challenges within the cybersecurity space are affecting society regardless of individual's level of education or technical background. Cybersecurity incidents are costing (losses) the economy thousands of rands annually. Hence, urgent measures have to be put in place to build resilience and reduce vulnerabilities in the cybersecurity landscape.

Given the increasing frequency and sophistication of cyber threats, this policy brief addresses the urgent need for a comprehensive approach to cybersecurity in South Africa, emphasising the importance of robust frameworks to protect critical infrastructure. Key recommendations include the establishment of a centralised oversight mechanism for critical infrastructure, significant investment in skills development, and the fostering of international collaborations to adopt best practices and share resources. The successful implementation of these policies will not only safeguard national security, but also align with Science, Technology and Innovation (STI) priorities for high-technology industrialisation, ICTs and smart systems.

Against the pace of development in the ICT space, there is a pressing need for the effective utilisation of Technical and Vocational Education and Training (TVET) and Community Education and Training (CET) colleges. These institutions are strategically located close to rural villages, making them accessible to a broader population. An intensive roll-out of ICT-related training could serve as a panacea for balancing the demand and supply of these scarce skills in the market, as all sectors – civil society, government and business – require them.

Introduction

In the recent past, South Africa has witnessed a significant increase in cyberattacks, affecting critical infrastructure, businesses, and individuals. This rise in cyberattacks in South Africa poses a growing threat to national security, economic stability, and the privacy of its citizens. Due to the prevalence of cyber threats, STI priorities outlined in the decadal plan – ICTs and Smart Systems, along with high-technology industrialisation – are being compromised. Furthermore, cyberattacks in South Africa undermine multiple Sustainable Development Goals (SDGs), including SDG 1 (No Poverty), SDG 3 (Good Health and Well-being), SDG 4 (Quality Education), SDG 8 (Decent Work and Economic Growth), SDG 9 (Industry, Innovation, and Infrastructure), and SDG 16 (Peace, Justice, and Strong Institutions) by disrupting essential services in health, education and obstructing progress across these critical areas. When SDGs and STI priorities are compromised, it leads to economic stagnation and diminished quality of life for citizens. This is a result of disrupted services and reduced growth opportunities.

The National Cybersecurity Policy Framework (NCPF) was established to improve South Africa's ability to prevent and respond to cyber threats. While progress has been made under the (NCPF), gaps in enforcement continue to persist. This policy brief seeks to propose strategies to strengthen South Africa's cybersecurity resilience. The recommendations focus on reviewing and updating the NCPF legislative enforcement, centralising oversight of critical infrastructure and the development of a skilled cybersecurity workforce.

Research approach and method

This policy brief stems from an in-depth analysis of existing data sources, such as strategies, annual progress reports, and other official publications of the relevant entities and respective policies and strategies. Through the in-depth synthesis and analysis of these selected documents, essential and unique knowledge, insights, and dynamics have been identified and appreciated.

Overview and implications of cybersecurity incidents

Cyberattacks in South Africa have increased in frequency and sophistication, posing significant risks to private businesses, public institutions, and the public. For example, data revealed a 22% year-on-year increase in ransomware incidents targeting South African institutions (Interpol, 2021). Cyber incidents are ranked as the second most dangerous risk in South Africa (Allianz Risk Barometer, 2023). Common cyberattack types include:

- **Phishing attacks:** Fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information.
- **Digital extortion:** Victims are tricked into sharing sexually compromising images which are then used for blackmail.
- **Business email compromise:** Criminals hack into email systems to gain information about corporate payment systems and deceive company employees into transferring money into their bank accounts. First National Bank, Standard Bank, and Nedbank have been targets of business email compromise and hacking. In February 2020, more than 1.7 million user accounts were hacked into at Nedbank. However, because of the sensitivity of cybersecurity, not much information was provided in the Nedbank cyberattack to demonstrate the extent of damages (Isa 2020; Dixon and Balson, 2020).
- **Ransomware:** Cybercriminals block the computer systems of hospitals and public institutions, then demand money to restore functionality (Khan et al., 2020).
- **Botnets:** Networks of compromised machines are used as a tool to automate large-scale cyberattacks (Interpol, 2021).

The African region experienced attacks against critical infrastructure and frontline services during the pandemic. This was most prominently observed in South Africa and Botswana. Interpol’s partner, Trend Micro (2021), recorded millions of threat detections in Africa from January 2020 to February 2021:

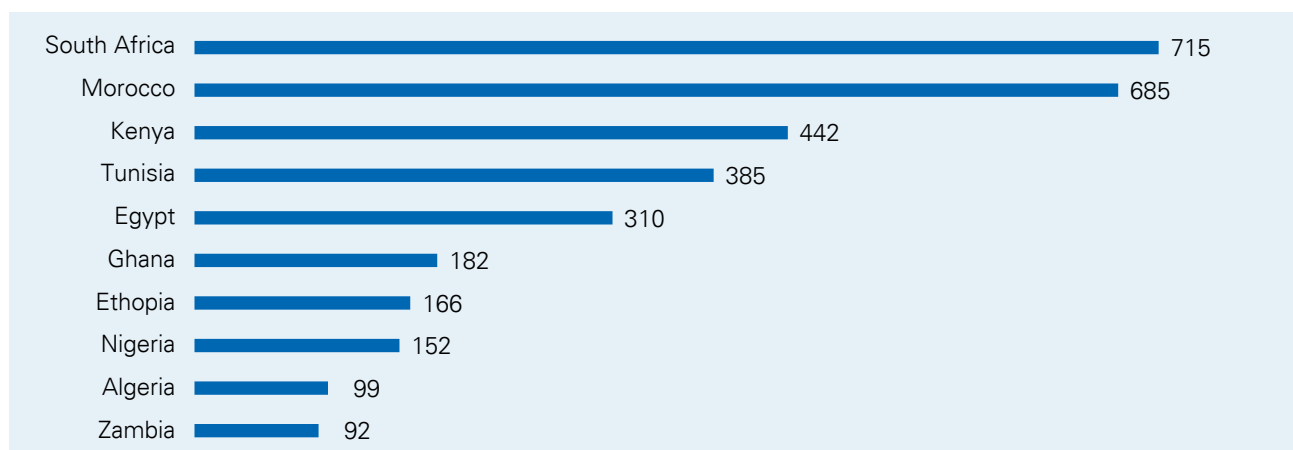
- **Email:** 679 million detections
- **Files:** 8.2 million detections
- **Web:** 14.3 million detections.

South Africa had 230 million threat detections in total (Trend Micro, 2021). In 2019, South Africa ranked third in cybercrime victims, losing R2.2 billion annually. By 2025, global cybercrime losses could reach \$10.5 trillion, with South Africa making a significant contribution.

A 2024 Allianz report ranked South Africa 14th for data breaches, with an average recovery cost of R49 million per attack.

South Africa is estimated to suffer 577 malware attacks per hour. Such malware attacks are among the emerging threats (Interpol, 2021).

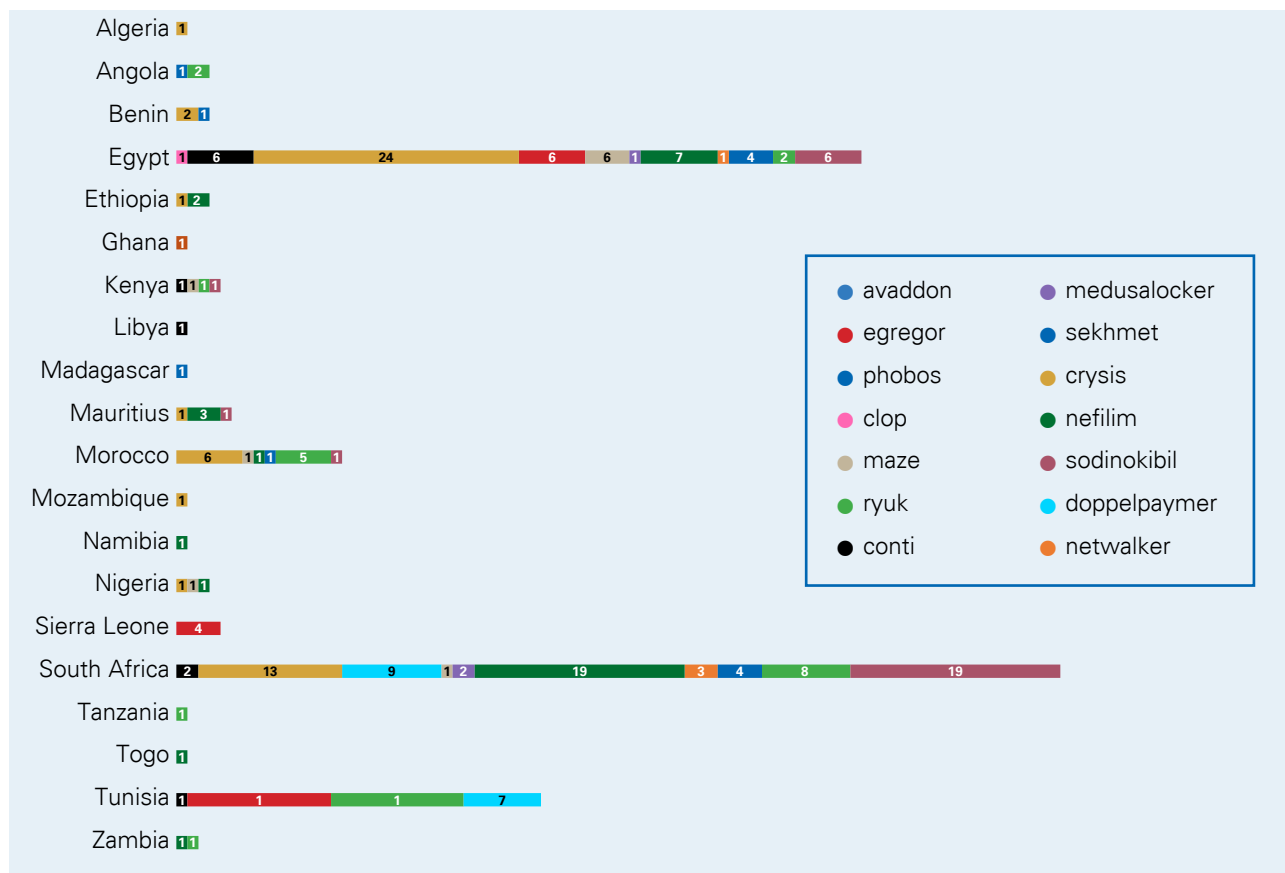
Figure 1: Number of unique IP addresses associated with digital extortion



Source: BusinessTech (2021)

The graph in Figure 1 illustrates the number of unique IP addresses associated with digital extortion scams in various African countries from January 2021 to May 2021, with South Africa having the highest count at 715.

Figure 2: Countries affected by ransomware



Source: Business Tech (2021)

Figure 2 above shows that South Africa was most heavily affected by targeted ransomware in the first quarter of 2021. Various ransomware families, such as Crysis, Nefilim, Ryuk, Clop and Conti, were prominently involved.

Table 1: Examples of data breaches in South Africa

Year	Organisation	Cause	Impact
2019	City Power	Ransomware	Power supply disrupted
2020	Life Health Care Group	Cyberattack	Disrupted admissions, processing systems and email servers
2021	Transnet	Ransomware	IT systems crippled; operations impacted
2021	Department of Justice and Constitutional Development	Ransomware	1 200+ confidential files
2023	South African National Defence Force	Claimed by Snatch threat group	Potentially massive data breach
2024	Tshwane University of Technology	Ransomware caused by Rhydsida group	Thousands of records stolen

Cybersecurity significantly impacts Sustainable Development Goals (SDGs) and Science, Technology, and Innovation (STI) priorities. Regarding STI priorities, cyberattacks disrupt digital infrastructure, hindering the deployment of innovative smart technologies and progress in ICTs and Smart Systems. Additionally, these threats can damage industrial systems and processes, slowing down the growth and advancement of high-tech industries.

Regarding the SDGs, cyberattacks undermine various aspects of development. They disrupt financial systems and social services, exacerbating economic inequalities and limiting resource access (SDG 1: No Poverty). Cyber threats also compromise patient data and disrupt healthcare delivery. The healthcare sector has also been targeted, with ransomware attacks jeopardising patient records and service delivery, thereby negatively affecting public health (SDG 3: Good Health and Well-being). The educational sector is not immune, as cyberattacks impact access to learning resources and disrupt educational continuity (SDG 4: Quality Education). Furthermore, recent cyberattacks on South African banks have resulted in millions of losses and compromised customer data, eroding public trust in digital financial systems. Additionally, attacks on critical infrastructure, such as ports, halt operations and disrupt key supply chains, undermining industry, innovation, and infrastructure (SDG 9). The erosion of trust in institutions, as seen in attacks on justice and defence systems, undermines governance, security, and justice (SDG 16). Additionally, the financial burden on businesses due to cybercrime, along with disruptions in e-commerce and online services, can result in job losses and hinder economic growth (SDG 8: Decent Work and Economic Growth). By crippling essential services, these attacks disproportionately impact marginalised communities that depend on digital services for healthcare, education, and social support.

Policy context and need for change

As a developing country with a good business infrastructure, South Africa has recently made notable progress in its cybersecurity policy landscape recently, with the National Cybersecurity Policy Framework (NCPF) at the heart of these efforts. The NCPF offers a unified strategy for securing cyberspace, detailing measures to protect critical infrastructure, establishing governance structures for cybersecurity, and promoting collaboration among the government, private sector, and civil society. Alongside the NCPF, the Cybercrimes Act (2021) represents a significant advancement by criminalising various cyber offences, including hacking and identity theft, and introducing penalties for cyber-related crimes. This legislation plays a crucial role in ensuring accountability, equipping authorities with the legal means to prosecute offenders and protect victims of cybercrime.

Nevertheless, South Africa continues to encounter significant challenges in achieving its cybersecurity objectives. Primary concerns include:

1. Non-implementation of the NCPF

The National Cybersecurity Policy Framework (NCPF) is not being effectively implemented, as evidenced by incidents like the 2021 hacking of the Department of Constitutional Justice (DC&J). This breach, resulting from the failure to renew essential cybersecurity tools, including the Security Incident and Event Monitoring (SIEM) licence, Intrusion Detection System (IDS), and antivirus software, highlights broader challenges in policy enforcement and resource allocation across government institutions. The establishment of a Cybersecurity Hub, as recommended by the NCPF, was intended to serve as a central resource for public and private sectors to exchange threat intelligence. However, it has faced hurdles due to insufficient funding and staffing. Furthermore,

the coordination among government departments and agencies has been inconsistent, resulting in disjointed efforts to tackle cybersecurity threats. This fragmentation has severely limited the country's capacity to respond promptly and effectively to cyberattacks, leaving it increasingly vulnerable.

2. Legal deterrence and punishment

Although South Africa has passed the Cybercrimes Act (2021), enforcement and legal frameworks are still catching up with the pace of cyber threats. Legal deterrence remains ineffective, and many cybercrimes go unpunished due to the complexity of tracking cyber criminals. There is a shortage of criminal justice experts knowledgeable about cyber-related cases (Ezeji et al, 2018).

3. Occupational skills shortage

In the annual Labour Market Research, the broad Information Communications and Technology (ICT), particularly network engineering, software development, data science automation and cyber security-related skills, are prominent among the scarce skills in the country. The NCPF emphasised the need for capacity building. Nonetheless, South Africa still faces a severe shortage of cybersecurity experts. The skills gap impedes the country's ability to defend against and respond effectively to cyberattacks.

professionals by 2025. A 2024 CSIR report indicated that 63% of cybersecurity roles in South Africa remain partially or fully unfilled. A report by Tredger (2023) highlights that about 64% of companies agree that the shortage creates more cyber threats. The skills shortage leaves South Africa exposed to attacks.

4. Exclusion of marginalised and vulnerable communities

Another significant gap is the exclusion of marginalised and vulnerable communities in the cybersecurity policy space (Gillwald and Mothobi, 2019). Given that a small number of existing capacities is concentrated in and serving urban centres, rural communities are at risk and more exposed to cyber security incidents. Many rural and economically disadvantaged areas in South Africa lack access to secure internet infrastructure, leaving them more susceptible to cybercrime.

5. Evolving cyber threat landscape

The global cyber threat landscape is always evolving significantly, and it has been almost a decade since the NCPF was approved. The policy appears to be based on earlier standards and may not fully address current developments and challenges.

6. Other contributing factors of cyber attacks

i. Increased digitalisation and remote work

The rapid shift to the use of digital platforms, caused by the COVID-19 pandemic, left many companies unprepared to secure their digital infrastructure. With more employees working remotely, hackers have found increased opportunities to exploit weak or inadequately secured home networks. This is largely because many companies did not have sufficient cybersecurity measures to handle a fully remote workforce (Accenture, 2022; WHO, 2020a; Quade, 2020; Simonovich 2020).

ii. Sophistication and the global nature of cyber threats

Cybercriminals are using increasingly sophisticated techniques in their attacks. Many of these originate from international cybercriminal networks, which poses significant challenges for South Africa in tracking and countering them. Some cybercriminals use South Africa as a testing ground before launching attacks globally. Furthermore, cybercrime tools and resources are now easily available on the dark web, enabling even amateur hackers to carry out attacks (Cisco, 2023; Khan et al., 2020; WEF, 2020;; WHO, 2020c).

iii. Old ICT infrastructure

All sectors are broadly affected, but some are impacted more than others. For example, due to the nature of the services they render to society, healthcare organisations (institutions) are particularly vulnerable to cyberattacks. The healthcare industry often lags in terms of cybersecurity, with outdated software and insufficient regulations. Healthcare facilities store a vast amount of confidential patient information, making them attractive targets for cybercriminals seeking to commit fraud and identity theft as there are readily available buyers for medical information. Additionally, the increased use of devices in healthcare organisations makes it challenging to stay on top of security measures (PwC, 2020; WHO, 2020a; Chigada, 2020).

Policy recommendations:

1. Review and strengthen policy

The Department of Communications and Digital Technologies (DCDT), the Cybersecurity Hub and the National Security Council or Relevant Government Committees must review the NCPF regularly and update the policy to ensure that it remains relevant.

2. Strengthening enforcement of the Cybercrimes Act (2021)

The Justice, Crime Prevention, and Security Cluster (JCPS), which oversees the implementation of the Cybercrimes Act, must be well resourced and capable of enforcing laws and policies. Furthermore, ongoing training for the judiciary and law enforcement is necessary to manage cybercrime cases effectively, ensure prompt prosecution, and act as a deterrent against cyber offences.

3. High level of investment in skills development

Given the spatial location of Technical and Vocation Educations and Training (TVET) and Community Education and Training Colleges (CET), South Africa needs to roll-out short-intensive vocational training programmes with the focus on closing the cybersecurity and associated skills gap. The shortage of skilled professionals is one of the most significant challenges facing the country's cybersecurity sector. To address this issue, the Department of Education (DoE) and the Department of Science and Technology (DSTI) must develop a national strategy to promote cybersecurity education, beginning at the primary and secondary levels and extending to university and technical training programmes. This includes the establishment of a policy to invest significantly in cybersecurity research, development and innovation. Public-private partnerships can play a crucial role in bridging this gap by providing internships, scholarships, and training initiatives. Additionally, partnering with countries that have advanced cybersecurity technologies and adopting global practices will facilitate resource sharing and the exchange of ideas, further enhancing efforts to minimise cyberattacks.

4. Public awareness

Enhancing public awareness and education on cybersecurity is crucial to reducing vulnerabilities, particularly among citizens and small businesses. A rolling-out of cyber awareness campaigns across the country is necessary, as well as cyber security training in government, business and non-governmental organisations. Many cyberattacks exploit human error, such as phishing scams or weak passwords. Therefore, a national cybersecurity awareness campaign, led by the Government Communication and Information System (GCIS) in collaboration with the private sector (including radio stations and print media houses) should be launched. This campaign should focus on educating the public about common threats, safe online practices, and the importance of data protection. Small and medium-sized enterprises (SMEs), which often lack the resources for advanced cybersecurity measures, should be specifically targeted with tailored training and accessible tools to improve their defences. By fostering a culture of cybersecurity awareness, South Africa can significantly reduce the risk of cyber incidents at the individual and organisational levels.

5. Centralised oversight of critical infrastructure

Strengthening the protection of critical infrastructure must be a top priority. As South Africa becomes more digitised, sectors like energy, finance, healthcare and transportation are increasingly dependent on digital networks, which makes them susceptible to cyberattacks. There must be a policy in place to identify national critical infrastructure and to develop centralised protection measures for these institutions to ensure a unified and strategic response to cyberattacks. Regular audits and security assessments of critical infrastructure should be required, with penalties for the sectors that do not comply. Additionally, developing real-time monitoring and incident response capabilities is essential to promptly addressing cyber threats and to prevent significant disruptions to essential services.

Conclusion

Above are some of the key areas that will help South Africa build cybersecurity and resilience for both society and the economy. Mainly, cybersecurity awareness must be made everybody's business, in that citizens must be empowered with information to the extent that they are confident in their ability to detect and act against cybersecurity threats. In addition, the government must make it mandatory for both large and small businesses, as well as non-governmental organisations, to invest in strengthening their cybersecurity defence measures (including hosting regular simulations) and reducing cyber risks. Overall, collective awareness and proactive actions will build resilience and a foundation of trust in the cybersecurity defence systems.

Author

Faith Tinonetsana, PhD: Policy Postdoctoral Fellow, National Research Foundation; Postdoctoral Fellow, Durban University of Technology

References

1. Accenture. (2022). Cyber Threat Intelligence Report: South Africa. Available at: Accenture's report on South African cyber threats
2. Allianz Global Corporate & Specialty. (2023). Allianz Risk Barometer: Identifying the major business risks for 2023. Allianz Group.
3. BusinessTech. (2021). *South Africa under cyberattack: Interpol reveals top threats in South Africa*. BusinessTech. Available at: <https://businesstech.co.za/news/it-services/531990/south-africa-under-cyber-attack-interpol-reveals-top-threats-in-south-africa/>
4. Chigada, J. (2020). 'Towards an aligned South African national cybersecurity policy framework', Unpublished PhD thesis, University of Cape Town, Cape Town
5. Greig, J. (2023). State-owned bank in South Africa confirms 'Akira' ransomware attack. *The Record*. Available at: <https://therecord.media/development-bank-of-southern-africa-akira-ransomware-attack>
6. Cybercrimes Act. (2021). Republic of South Africa. *Cybercrimes Act, No. 19 of 2020*. Government Gazette
7. Dixon, W. and Balson, D. (2020), *How COVID-19 shows the urgent need to address the cyber poverty gap*. Available at: <https://www.weforum.org/agenda/2020/03/covid-19-pandemic-shows-the-urgency-for-addressing-the-cyber-poverty-gap/>.
8. Ezeji, C. L., Olutola, A. A., & Bello, P. O. (2018). Cyber-related crime in South Africa: Extent and perspectives of state's role players. *Acta Criminologica: Southern African Journal of Criminology*, 31(3), 93–108.
9. Gillwald, A., & Mothobi, O. (2019). A demand-side view of mobile internet from 10 African countries. *Research ICT Africa*.
10. Institute for Data Science and Innovation. (2024). *A review of South Africa's national cybersecurity policy framework: Progress and challenges after nearly a decade*.
11. Interpol. (2020), COVID-19 cyberthreats. Available at: <https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats>
12. Isa, M. (2020) *SA suffers as cybercrime rises globally*. News24 Business. Available at: <https://fin24.com/Finweek/Business-and-economy/sa-suffers-as-cybercrime-rises-globally-20200106>
13. Kaspersky L. (2021). Ransomware attacks in South Africa. Available at: [Kaspersky's cybersecurity insights] (<https://www.kaspersky.com>)
14. Khan, N.A., Brohi, S.N. and Zaman, N. (2020). *Ten deadly cybersecurity threats amid COVID-19 pandemic*, IEEE. Researchgate publications, Berlin
15. National Cybersecurity Policy Framework (NCPF) Republic of South Africa. (2015). *National cybersecurity policy framework*. Department of Communications and Digital Technologies
16. SAnews. (2024). National health lab now fully operational after cyber attack Available at: <https://www.sanews.gov.za/south-africa/national-health-lab-now-fully-operational-after-cyber-attack>
17. PwC. (2020). Impact of COVID-19: The world has changed and so have we. Available at: <https://www.pwc.co.za/en/about-us/integrated-report-2020/impact-of-covid-19.html>.
18. Quade, P. (2020). A deep dive into the universe of cybersecurity: The digital big bang. World Economic Forum COVID Action Platform. Available at: www.weforum.org.

19. Simonovich, L. (2020). Are utilities doing enough to protect themselves from cyber-attack? World Economic Forum. Available at: <https://www.weforum.org/agenda/2020/01/are-utilities-doing-enough-to-protect-themselves-from-cyberattack/>
20. Tredger, C. (2023). *South Africa under pressure to fill cyber security skills gap*. ITWeb. Available at: <https://www.itweb.co.za/article/south-africa-under-pressure-to-fill-cyber-security-skills-gap/DZQ587V8bjrqzXy2>
21. Trend Micro. (2022). Navigating new frontiers: Trend Micro 2021 annual cybersecurity report.
22. World Economic Forum. (2020), *COVID-19 risks outlook: A preliminary mapping and its implications*. Available at: <https://www.weforum.org/global-risks/reports>
23. World Health Organization (WHO). (2020a). *Beware of criminals pretending to be WHO*, Available at: <https://www.who.int/about/communications/cyber-security>
24. World Health Organization (WHO). (2020c) *Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019–nCoV)*