The Advancement of 4IR Technologies and Increasing Cyberattacks in South Africa

Rabelani Dagada
https://orcid.org/0000-0002-3025-6678
University of South Africa
dagadr@unisa.ac.za

Abstract

The fourth industrial revolution (4IR) is an era characterised by accelerated technological progress. Even though access to 4IR technologies is not yet widespread, in the current era, 4IR technologies affect socio-economic activities and digital business. The pace of digital transformation also has some implications for cybersecurity. The purpose of this study was to assess the impact of these 4IR technologies on cyberattacks in South Africa. The study used qualitative data collection methods, namely, interviews and document collection. Purposive and convenience sampling were used to select the study participants. An analysis of the collected data yielded four major findings. A major tenet of these findings was that there is a correlation between the advancement of 4IR technologies and the rapid increase in cyberattacks in South Africa. The study has made theoretical and practical contributions as well as some essential contributions to digital transformation and cybersecurity theories. The findings and recommendations of the study can be used in other countries in southern Africa. One recommendation is for business executives to implement certain measures to strengthen cybersecurity in their organisations. Further, policymakers in South Africa are advised to ensure that public policies and law enforcement agencies are able to use advanced technologies to prevent and deal with cyberattacks.

Keywords: fourth industrial revolution; advanced technologies; digital business; digital transformation; cyberattacks; cybersecurity

Introduction and Background

As many authors have written, cyberattack activities worldwide are on the rise revealing instances of organised crime syndicates in full operation with huge success rates (Corallo et al. 2022). This profitability has encouraged these syndicates to advance their abilities and to increase their activities. People are exposed daily to both local and

UNISA
Southern African Journal of Security
#15157 | 27 pages
https://doi.org/10.25159/3005-4222/15157
ISSN 3005-4222 (Online)

international news on cyberattacks and, in some cases, their success in stealing from average consumers to corporate giants.

Crime associated with the use of networked computers is not new, in fact research on the subject can be found dating back to the 1970s (Campbell 2005). It is on this premise that since 2003, various countries have adopted cybersecurity awareness month. In March 2019, the then Deputy Minister of Communications in South Africa, Pinky Kekana, announced that South Africa was adopting October as its cybersecurity awareness month (Dagada 2021). A country can only do this when there is a high level of cyberattacks in its jurisdiction.

While cyberattacks were increasing in South Africa, the 4IR was also advancing. An extensive study needed to be conducted to determine if there was a correlation between these two phenomena. By 2015, there were more than 9 billion devices that were digitally connected worldwide (Diamandis and Kotler 2020). It is expected that this number will grow to between 25 billion and 50 billion by 2025 (Diamandis and Kotler 2020). Digitalisation is becoming ubiquitous and internet connectivity is starting to find its presence in everyday things like household appliances, food packaging, furniture, and vehicles. This should be attributed to the 4IR technologies.

Commerce at large – and digital businesses – have become beneficiaries of the ushering in of the 4IR. Its technologies have been transforming business processes and enabling innovative business models. The 4IR is synonymous with advanced innovations in artificial intelligence (Chaka 2023). This class of innovation includes virtual assistants, drones and translation software, along with self-driving cars that are increasingly becoming a common reality (Dagada 2021). All this is indicative that the fourth wave of the industrial revolution is a world of infinite possibilities and that it is leaning on automation of applications that are increasingly devoid of human participation. Indeed, this is a giant leap for humankind, from depending on horses for transportation in the first industrial revolution to having access to driverless cars in the 4IR (Othman 2022).

Three megatrends define the 4IR, namely, the physical, digital and biological trends. The physical trends are subdivided into four manifestations, namely, autonomous vehicles, 3-D printing, advanced robotics, and new materials (Schwab 2017). While 4IR technologies have been growing exponentially and adding value to digital business – cyberattacks have also been growing rapidly. The current study investigated whether there was a correlation between these two phenomena in South Africa. The advancement of 4IR technologies in South Africa has inadvertently led to an increase in cyberattacks. As a result, individuals and businesses must protect their information from attackers or competitors as loss of information could lead to lawsuits or loss of business. This protection can be achieved by fortifying cybersecurity.

Hacking is one of the most well-known types of cybersecurity-related risks and crimes (Dagada 2021; Maiwald 2004). Simply put, hacking involves breaking into information

systems to make them dysfunctional or to steal information for whatever purpose. Malicious code, widely known as malware or viruses, is one of the major cyberattacking techniques (Dagada 2013). According to Maiwald (2004, 67), the term "malicious code" refers to computer viruses, Trojan horse programs, worms, and others. Together they are called "malware" (Dagada 2021). Just as in the biological field, it is difficult to contain computer viruses.

Research Problem

While many studies have been conducted related to information security in South Africa by scholars – such as Sutherland (2017), Gcaza and Von Solms (2017), Mabunda (2021), Netshakhuma (2023) and others – it remained to be established whether there was a correlation between the advancement of 4IR technologies and the rapid increase in cyberattacks in South Africa. There was a gap in the literature regarding this matter. The literature did not show if organisations and governments in the country were satisfactorily dealing with the increasing cyberattacks. The lack of research seemed to indicate the need for research in this field. Having said that, there is a substantial body of literature that indicates that cyberattacks have been increasing rapidly both globally and locally.

Purpose of the Study

The purpose of the study was to investigate the advancement of 4IR technologies and increasing cyberattacks in South Africa. The following research questions were used to guide the study, namely:

1. To what extent does the advancement of 4IR technologies affect the rate of cyberattacks in South Africa?
2. What are the measures employed by organisations in South Africa to deal with the increasing cyberattacks?
3. What are the measures employed by the government and its law enforcement agencies to deal with the increasing cyberattacks?
4. What is the impact of legislation in South Africa in combatting the increasing cyberattacks?

Fourth Industrial Revolution Technologies

The first industrial revolution was characterised by the primary forms of production such as agriculture, mining, and extractive economic activities; the second industrial revolution related to mass production, manufacturing, mechanisation, and electrical power; while the third industrial revolution (also known as the digital revolution) was dominated by the services sector (information technology, retail, management consulting, media, entertainment, etc.) (Fourie 2021). The first industrial revolution started about 10 000 years ago; the second industrial revolution around 1870; and the third industrial revolution around the 1950s.

The services sector is currently being succeeded and complemented by the 4IR, and it is synonymous with the innovative convergence of old and new technologies, involving the physical, digital, and biological realms (Diamandis and Kotler 2020). It builds on the third industrial revolution and began at the turn of the 21st century. Its major features are: a mobile internet connection; the use of small but powerful sensors; the availability of increasingly cheaper applications; artificial intelligence (AI); machine learning; blockchain; the internet of things (IoT); quantum computing; advanced robotics; autonomous vehicles; virtual reality; augmented reality; the metaverse; and flying cars (Dagada 2021). Digital technologies that are anchored on hardware, and use software and networks, are not necessarily new; but what differentiates them from the third industrial revolution is that the current one is more sophisticated and integrated (Diamandis and Kotler 2020).

Consistent with this worldview, Massachusetts Institute of Technology luminaries, Brynjolfson and McFee (2014), identify the current age as the "second machine age", and this is out of recognition of the role of a technology revolution. Thus, the foundation of the 4IR is the primacy of autonomous technology and the relegation of the dependency on human sustenance (Dagada 2022a). Therefore, much as the previous industrial ages were characterised by humans interacting with machines, the contemporary age is mostly about what technology can do without the extreme dependence on human muscles. This is further accentuated by simultaneous developments in the life sciences subsector (e.g. gene sequencing); breakthroughs in nanotechnology; and quantum technology (Diamandis and Kotler 2020). In this realm, the fourth wave of the industrial revolution is characterised by new inventions as well as improvements of earlier technologies – and all these converging and interacting across the physical, digital and biological realms (Schwab 2017).

Dagada (2022a) asserts that the 4IR is expanding faster and touching human lives quicker than the previous three revolutions. In contrast to the previous revolutions (from the first to the third), the 4IR is expanding rapidly and is not mutually exclusive to other disciplines (Diamandis and Kotler 2020). Instead, it encourages the harmonisation of disciplines, discoveries, innovations, and scientific realms. It follows that various technologies and services have converged, including the following: computing, gaming, wireless, and wireline communications conduits, consumer electronics, digital media, print media, broadcasting, publishing, gaming, socialising, and photography (Dagada 2021). This list is not exhaustive. Convergence refers to the blurring of lines between technologies and delivery channels. 4IR technologies include the following: AI, blockchain, the IoT, advanced robotics, autonomous vehicles, quantum computing, sensors, 3-D printing, augmented reality, virtual reality, machine learning, and the metaverse. The 4IR technologies are quickly becoming integrated into the three previous waves – the primary forms of production (agriculture, fishing, hunting, finishing, mining, and other extractive economic activities); the secondary form of production (manufacturing); and the tertiary sector (financial, retail, information and communication technologies (ICT), tourism, health, and other services). Within the next

10 years, 4IR technologies will become ubiquitous (Dagada 2021; Fourie 2021). Five factors are increasing the pace of the integration of 4IR technologies into all economic sectors and almost all spheres of human lives, namely: acceleration, deception, disruption, demonetisation, dematerialisation, democratisation, and new business models. The study found that while these developments are impressive, they must contend with increasing cyberattacks and are also in fact leading to the increment of cyberattacks. More details regarding this are contained in the section dealing with the findings of the study.

Cybersecurity at a Glance

This section deals with the brief evolution of the internet and the World Wide Web; the emergence of digital transactions; and cybersecurity for confidentiality, integrity and availability.

Cybersecurity

It has been stated previously that digital business is growing fast. It does seem, however, that one of the major obstacles to a more rapid growth of digital payment has been customer concerns regarding cybersecurity-related issues (Mijwil et al. 2023). It should also be noted that, from the start, the internet was designed to share information and not to hide it (Dagada 2013). At that stage, it did not seem to be necessary to build in tight cybersecurity features since it was taken for granted that all transmissions would be carried over private lines. Top secret military transmissions are still on private networks, but the basic technology has moved to the world's public network – the internet and companies' internal networks (Mijwil et al. 2023). It is here that consumers and merchants find themselves using protocols that were primarily designed for connectivity and going over inherently public and corporate networks where there is a serious "lack of sentries guarding the gates" (Crume 2000).

A major concern in digital business has been cybersecurity for confidentiality, integrity and availability as outlined below.

Cybersecurity for Confidentiality

It has been stated in this section that credit and debit cards, EFTs, and other electronic payment methods are some of the electronic payment methods in a digital business environment. One of the major impediments to the general use of these digital payment methods in digital business transactions has been the concern in some consumers' thinking that they lack sufficient confidentiality (Corallo et al. 2022; Dagada 2013).

Cybersecurity for Integrity

One of the problems of using cyberspace for commercial purposes is its questionable integrity. It is here that some marketers find it difficult to convince consumers to buy their products and services online (Jackis and Abass 2019). On the other hand, some

consumers would not even bother to consider an online advertisement due to integrity concerns. This has led consumers to only trust established online retailers (Corallo et al. 2022). The consequence of this is that small, micro and medium enterprises end up suffering huge losses.

Cybersecurity for Availability

One of the major challenges facing online retailers is to secure the availability of their digital business websites consistently (Saura, Palacios-Marques and Barbosa 2023). The unavailability of a particular website could be due to an attack. According to Fang and Qureshi (2014), attacks on availability are designed to prevent legitimate users from using an online resource such as digital banking. The digital revolution is expanding rapidly due to digital business (Jackis and Abass 2019). It is on this premise that most organisations are striving to catch up. De Kare-Silver (2001, 44) noted more than two decades ago that it was a daunting task for organisations to master the new environment, explaining that: "There is a new game in town, and it is now about learning and embracing the new factors for success". These words are now even more applicable in digital business (Dagada 2022a).

According to Ghimire and Rawat (2022), the challenges brought by the internet to the corporate environment are exacerbated by cybersecurity risks, threats and crime. Although cybersecurity is essential to be able to use information resources, it is not just cybersecurity that organisations need to achieve (Mijwil et al. 2023). Users should be able to trust the infrastructure on which they rely to facilitate their private and business transactions. Be that as it may, trust in digital business is a product of dependable cybersecurity. Dagada (2013) declares that cybersecurity is a digital business's Achilles heel. The business-to-consumer component of digital business may be affected by reservations regarding cybersecurity breaches. Credit card is the most common online payment option and thus both digital business customers and merchants are vulnerable to potentially high levels of fraud due to stolen cards and illegally acquired card numbers (Mijwil et al. 2023).

Although new technical techniques are constantly being developed to deal with cyberfraud, these techniques are not necessarily fool proof, and a perfect method of encrypting has not yet been developed. It is because of this premise that cybersecurity measures cannot be left to technical techniques only. Physical security and digital governance measures should be implemented (Dagada 2021). Similarly, dealing with cybercrime also cannot be left only to organisations in the corporate environment. According to Campbell (2005) and Dagada (2021), several governments have developed legal requirements regarding digital business. The challenge is how to regulate digital business activities through national regulation since the internet transcends geographical boundaries. Some governments are stricter than others, but they do not have the right to impose their laws and standards on other countries. South African digital business merchants and consumers are not immune to cybercrime (Dagada 2013). To this end, the South African government promulgated the Electronic

Communications and Transactions (ECT) Act 25 of 2002. Both the King II report of 2002 and King III report of 2009 contained good governance recommendations that dealt with cybersecurity issues. Before the ECT Act and the King II Report, South African digital business merchants and customers relied on common law (Dunlop 2005). The legislation that was introduced through the ECT Act has somewhat given digital business participants confidence in transacting over cyberspace (Dagada 2021).

Research Methodology

The fieldwork for the study took place from 7 April 2021 to 5 May 2023. This section deals with the research approach, sampling, data collection techniques, data analysis, trustworthiness of the study, and ethics. The study employed qualitative research methodology. This methodology was useful in testing the research questions and sub-questions of the study. The 25 study participants also constituted a rich and valuable source of information. The study went "beyond numbers" and statistics (Greenhalgh and Taylor 1997, 741). It took the form of a generic study to examine the impact of 4IR technologies on the rate of cyberattacks. The study participants were business executives, cybersecurity practitioners, academics, and other relevant experts. Convenience and purposive sampling were used to select the participants. It was inexpensive and convenient to interact with them because they were all based in South Africa and most of them had access to online meeting platforms such as MS Teams or Zoom.

Convenience sampling as applied in the study might not assure an impartial representation of the South African situation. This perceived limitation was mitigated by purposive sampling (Kenny, Doyle and Horgan 2023). The participants were also chosen on purpose because of the perceived contribution that they could make to the study. According to Truman (2023), the strength of purposive sampling is based on the selection of those participants who will narrate data-rich cases for an in-depth study. Data-gathering methods that were used in the study were interviews, document collection and analysis thereof. Semi-structured interviews were conducted with the participants. This made it possible to get hold of information from the numerous informants. Interview protocols were employed to gather data and to provide responses to the research question and its sub-questions.

The interview is a particularly suitable data-gathering method for the environment concerned and made it possible to collect valuable information concerning the research questions. This provided me with an opportunity for direct exchange with the study participants and enabled me to obtain facts directly from them. The data gained from the interviews was analysed using open coding (Li and Zhang 2022). A recurrent comparative method was applied to analyse data within and between interviews. Content analysis was also applied to analyse the content of interviews (Merriam 1998). The process entailed the instantaneous coding of raw data and the formation of categories. The data was analysed to discern common patterns and to put together

categories. These categories were weighed against the literature and were used to answer the research question and its sub-questions. The data collected through document analysis was analysed by matching it up with the data collected from the interviews, and through content analysis.

The trustworthiness of the study was based on two fundamental criteria, namely, validity and reliability (Paulus 2023). Validity is the extent to which the research instrument tests the actual object or subject of measurement. There are two forms of validity: internal and external. Reliability, on the other hand, is assessing the accuracy and precision of the research instrument. The study employed multiple data collection techniques and gathered information from various sources. This satisfied the principles of triangulation and went along to ensure the reliability and validity of the study (Paulus 2023; Shrivastava and Shrivastava 2023). Some organisations and people participating in the study were allowed to examine the evolution of the research report as it was being written up. This made it possible for them to identify information that might not have been a true reflection of what was observed, read, and/or said during the fieldwork. This approach is supported by Schoonenboom (2023). Ethical aspects were observed in the study even though some readers may not perceive the study as being sensitive work.

The participants were requested to contribute to the study via e-mail. All the participants agreed to take part in the study by providing written approval. They also agreed to the recording of discussions during data gathering. I coded the audio-recorded conversations and put the recordings in a password-protected computer and a locked facility. The participants were at liberty to withdraw from the study at any time without being required to give a reason. All necessary measures were taken to guarantee that the study participants were not caused any harm by participating. Therefore, fictitious names were used to protect their identity and to make sure that any information, either personal or professional, revealed during the interviews was handled as confidential. Ethical clearance was obtained from the University of Johannesburg's Faculty of Humanities Research Ethics Committee.

Study Findings

An analysis of the data generated four major findings, namely: that 4IR technologies have led to the increase of ransomware in recent years; that Covid-19 led to the increased use of 4IR technologies, and the escalation of cyberattacks; that 4IR and its convergence of technologies has led to the increase of cybercrime; and that government and corporate South Africa are largely inadequately equipped to deal with cyberattacks. The quotes have been taken verbatim from the interviews with the study participants.

4IR Technologies Have Led to the Increase of Ransomware in Recent Years

The system engineer said that:

> Since 2018, we have observed a surge in ransomware attacks both locally and abroad. There is no doubt this is linked to the advancement and increased use of 4IR technologies.

Ransomware is a type of malicious software that enables cyberfraudsters to gain unauthorised access to an organisation's information systems and threaten to either publish or permanently block access to the information unless a ransom is paid (Dagada 2021). Locally, organisations such as Liberty Holdings, the City of Johannesburg, ViewFines, the Master Deeds Office, Omnia Holdings, Life Healthcare, Momentum, Nedbank, and a few other banks have been victims of ransomware attacks. One of the local insurance services powerhouses, Liberty Holdings, became a victim of ransomware in June 2018. The manager of the security operations centre explained that:

> A certain external party was claiming to have captured data from the insurer and demanding a ransom payment. Some media outlets reported that hackers were able to have access to sensitive data of some of the insurer's top clients. Fortunately, Liberty was able to secure its information systems.

Although no financial losses were reported, this incident made a huge dent in the insurer's reputation. The matter was so serious that the then CEO of Liberty Holdings, David Munro, had to convene a press conference on a Sunday evening (17 June 2018) to allay the fears of the insurer's stakeholders and to protect the value of its share price.

Although the cyberhackers did not steal any money, in the text messages that the life insurer sent to its customers, it acknowledged that its systems were illegally accessed. The text partially revealed that it had "been subjected to unauthorised access to its IT infrastructure, by an external party". The senior cybersecurity advisor made the following observation:

> The market took this incident seriously. Liberty Holdings share price dropped by 4.7% and R1.68 billion was wiped out of the company's R34 billion market value in the next two days after the attack.

At the above-mentioned press conference, Munro said that an email repository had been compromised and the cyberfraudsters, who were not identified, had demanded a ransom. The business analyst noted that:

> Instead of acceding to this demand, the insurer called in cybersecurity and forensic experts who countered the cyberattack and the breach.

Munro also confirmed at the press conference that there were neither funds stolen nor ransom paid. The executive head responsible for the network operations centre observed that:

> Be that as it may be, there is no doubt that this breach exposed the personal information of millions of its customers and those insured.

The Liberty Holdings breach was significant because it was the biggest victim of ransomware among major financial services companies in South Africa. Before this, a small financial services provider, Postbank, was hacked, and some money was stolen. Ransomware became famous in May 2017 when it was used to freeze the operations of one of the large couriers – FedEx, Russia's Interior Ministry, British national health-care service, French car manufacturer – Renault, and Spain's biggest telecommunications network provider – Telefonica (Dagada 2021). In the Liberty Holdings ransomware, it was suspected that the hackers took advantage of the email repository because it could have been less heavily secured than other information systems. As one analyst put it, one thing good about this incident was that it demonstrated the extent to which emails were unsecured. The email system was initially established to send basic text messages through the nascent network that later evolved into the internet and the World Wide Web (Dagada 2013). It has now developed into a backbone of global communications. The IT operations manager explained as follows:

> The availability of email systems is not just a gift to people and corporates, but it is also a gift to the cybercriminals who only need to penetrate our email inboxes to gain access to the most critical ICT infrastructure.

Email system vulnerability is exacerbated by the fact that it is usually the first facility for password resetting. Once this avenue has been compromised, a cybercriminal can reset passwords to various services (Dagada 2013).

Worse still, by the end of the first half of 2020, the South African government had not yet implemented all the provisions of the Protection of Personal Information (PoPI) Act 4 of 2013 which would provide consumers with extra security against breaches of their data – on top of the reputational damage caused in such breaches. Email is a distinct example of the trade-off consumers are compelled to make between convenience and protection. Before the Liberty Holdings cyberattack, the ViewFines data breach incident took place in South Africa wherein the personal details of about 1 million people were exposed. The platform, ViewFines.co.za, enabled participating South Africans to pay their road infringement fines online. The digital platform was taken offline after the cyberattack. Another ransomware attack involved the breach of the Master Deeds Office in 2017 when property company Jigsaw posted an estimated 60 million personal details on the web in an unsecured database. After this, the City of Johannesburg and local banks were subjected to cyberattacks in October 2019. The cybersecurity specialist said that:

> In the City of Johannesburg hackers breached IT systems and the city responded by shutting down its email system, websites, e-Services, and other digital platforms as a precaution. This occurred after a 4.0 bitcoin ransom demand from a group of cybercriminals called Shadow Kill Hackers after they had gained unauthorised access to the city's digital platforms.

At the same time, several banks in South Africa also reported that their digital services were experiencing problems and they believed it had something to do with the ransomware attack attempts.

In February 2020, the banking group, Nedbank, reported that a cybersecurity breach at one of its third-party service providers led to the data of around 1.7 million of its customers being accessed and compromised. This service provider was responsible for direct marketing on behalf of the bank and other clients. In February 2020 and June 2020, fertiliser maker – Omnia Holdings, and private hospital group – Life Healthcare, were targets of cyberattacks. The World Economic Forum estimated that South African companies lost about R5.8 billion in 2015 because of cybercrime (Dagada 2021). The same organisation mentioned cybercrime as one of the three biggest threats confronting Africa in 2019 and years beyond. The professor of commercial law asserted that:

> As ransomware attacks increase both in South Africa and worldwide, we must ask ourselves as to whether local companies are sufficiently armed against these attacks. A review of several cyberbreaches suggests that South African companies are not adequately equipped to guard against cyberattacks.

This was confirmed by the Cyber Exposure Index in September 2021. This index ranks countries according to the number of companies that suffered cyberbreaches – South Africa was the sixth most exposed country for cyberattacks in general and ransomware. According to the consultancy house, Accenture, South Africa has the third-highest number of cybercrime corporate victims in the world, with banks being the biggest targets (Gavaza 2020). The chief technology officer indicated that:

> In May 2020, one of the big credit bureau agencies, Experian, became a victim of a massive ransomware attack. This exposed the personal information of about 24 million people in South Africa, and the business information of up to 800 000 companies. Data obtained from the Experian breach were dumped on the websites and online forums, and it was publicly viewable.

Experian only reported the breach to the Information Regulator South Africa months after the cyberattack. This ransomware attack took place two months before the PoPI Act came into effect. At the time, the massive breach occurred and was reported to the regulator, Experian was not liable to the PoPI Act because organisations still had up to 1 July 2021 to comply with the Act's various obligations. News about the Experian cyberbreach came later in August 2020 after the insurer, Momentum, was cyberattacked. The insurer had to inform its stakeholders that hackers had access to a portion of its data. Since the PoPI Act became effective on 1 July 2021, companies that do not comply with its provisions, irrespective of whether it is accidental or intentional, are subjected to severe penalties. The Act stipulates fines of up to R10 million, and a maximum jail sentence of 10 years, depending on the gravity of the data breach (Dagada 2021). In July 2021, a South African state-owned entity, Transnet, became a victim of ransomware. Banks and other enterprises in South Africa should, among others, also

employ traditional old-fashioned methods like hardening their email systems to tighten the security of their digital platforms. There is no doubt that banks and other financial institutions will increasingly use AI, robotics, the IoT, and other advanced technologies to counter cybercrime (Dagada 2021).

Covid-19 Led to the Increased Use of 4IR Technologies and the Escalation of Cyberattacks

There has been a tit-for-tat strategy between Russia and the United States (US) wherein the two nuclear superpowers accuse each other of cybercrime operations on critical infrastructure. The adjunct professor explained as follows:

> The US has gone a step further and also blamed China's Ministry of State Security for sponsoring hackers who execute illegal cyber operations internationally as part of sovereign spying, industrial espionage, and personal profit through ransomware.

Owing to severe measures taken by President Cyril Ramaphosa's administration to contain the Covid-19 pandemic in South Africa and the restrictions on people's movements for socio-economic purposes, there was increasing usage of digital platforms for social, educational and commercial purposes. Consequently, cyberattacks increased rapidly and substantially in South Africa. A reputable company that specialises in cybersecurity, Kaspersky, reported that since President Ramaphosa declared a state of disaster on 15 March 2020, South African organisations have experienced an unprecedented increase in cyberattacks. The company indicated that towards the end of March 2020, cyberattacks had gone up tenfold from 30 000 devices affected daily before Ramaphosa's announcement to 310 000 devices in the days that followed.

In its statement issued in March 2020, the South African Banking Risk Information Centre (SABRIC) advised South Africans to be vigilant as it also expected an upsurge in digital banking fraud. The managing executive of Digital Banking observed that:

> Recent cyberattacks ranged from fake charities and phishing scams, and malicious websites to spam emails. During the height of Covid-19, cyberattacks came in the form of spoofed emails offering products that would help to prevent infections. These included gloves, masks, and vaccines.

The spike in cyberattacks could be attributed to school-going learners, university students, and professional workers working remotely based in their homes. Most of these digital platform users did not have sufficient security measures.

Assertions made by interviewees Kaspersky and SABRIC were confirmed by the European Union (EU) and the European Union Agency for Law Enforcement Cooperation (Europol). The surge in cybercrime during the Covid-19 lockdowns, state of disasters, or state of emergencies was not confined to South Africa; it was a

worldwide phenomenon. Ursula von der Leyen, who served as the European Commission president, warned in March 2020 that cybercrime in the EU had jumped up owing to the Covid-19 outbreak (Dagada 2021). She said that cybercriminals were taking advantage of the increased amount of time that people were spending on digital platforms owing to measures taken by various countries to curtail the spread of the coronavirus. These criminals followed people on digital platforms and exploited their concerns about Covid-19, thereby causing their vulnerability to become a commercial opportunity for cybercriminals. It was on this premise that Europol increased its fight against trafficking in counterfeit Covid-19 medicines. The European Association of Computer Security Incident Response teams, and the World Health Organization (WHO), also warned people and companies to enhance their level of alert and cybersecurity during this period. The chief risk officer indicated that:

> Authorities had also observed that telecommunications networks, research hubs, hospitals, and medical centres were also targets of cyberbreaches. Cybercriminals were attacking these facilities so that they would gather more information and intelligence.

Organised units of cybercriminals also tried several times to gain accessibility to the WHO's digital networks and those of its partners during the height of Covid-19. The aim of attacking the digital systems of prominent health organisations during the pandemic could have been to get information about tests, vaccines and cures related to Covid-19 so that the criminals could sell these on the black market. Most importantly, intelligence gathered through the hacking of digital systems of reputable health organisations would enable cybercriminals to deceive and defraud systems users who were mostly working from home.

These assertions were supported by credible local and international organisations. In its press statement released on 27 March 2020, Europol reported that factors prompting a spike in cybercrime during the pandemic included the following: high demand for certain goods, protective gear and pharmaceutical products; decreased mobility and flow of people across and into the EU; citizens remaining at home and increasingly teleworking, relying on digital solutions; limitations to public life made some criminal activities less visible and displaced them to home or online settings; increased anxiety and fear that may create vulnerability to exploitation; and decreased supply of certain illicit goods in the EU. Cybercriminals used the Covid-19 crisis to carry out social engineering attacks under the guise of the pandemic to disseminate various malware packages. An overriding theme in all these was that cybercriminals were taking advantage of school-going learners, university students and professional workers working from home and connecting to their organisations' digital platforms remotely via wireless networks.

It took many months for the authorities to develop a vaccine and mitigate against the Covid-19 pandemic. This would entrench the culture of physical distancing, studying and working from home in South Africa. For various reasons, before the outbreak of

Covid-19, South African employers and employees were latecomers to the phenomenon of working from home. Resistance by both some companies and employees to embark on remote working, also called telecommuting, had left South Africa five years behind the curve. Most employers in South Africa felt very strongly that their staff must be seen at the workplace during working hours regardless of the quantity and quality of their output. If managers in these companies could not see their employees working, it meant that they were not working. There was also a mindset among most South African workers of togetherness; they shunned the idea of a solitary working environment in their home, library or local coffee shop. The senior cybersecurity advisor observed that:

> The crisis brought by the Covid-19 pandemic and the drastic measures taken by the government to limit the infection rate, served as strong culture shock that forced schools, universities, pupils, students, employers, and employees to embrace studying and working from home by accessing their organisations' digital systems.

Covid-19 led to the increased use of 4IR technologies. When it came to employers and employees, this new reality took hold, and it became difficult to turn back the clock despite the availability of vaccines and substantial reductions in new Covid-19 infections and deaths. Working and studying from home have become rooted in society, and this has been a major boost to the use of 4IR technologies. Most employers and learning institutions have adopted a hybrid model in which employees sometimes have to go in to their offices and learners to the campuses. Unfortunately, an unintended consequence of this phenomenon is that it has led to an increase in cyberattacks. The professor of commercial law declared that:

> After the 1918 Spanish flu pandemic, global and local economies were devastated. In South Africa, life insurance, which was not prominent before the Spanish flu, became one of the most dominant sectors. During this post-Covid-19 era, we are witnessing the growth of some advanced technologies. These include technologies that enable people to work and study from home while being able to collaborate with their mentors and colleagues.

Again, as indicated earlier, the upshot of this situation has been a substantial increment in cybersecurity attacks, and therefore, much should be done to strengthen cybersecurity.

4IR and Its Convergence of Technologies Has Led to an Increase in Cybercrime

The chief security advisor made the following comment:

> Most of us cybersecurity practitioners have witnessed the increase of cyberattacks in South Africa in recent years. This should be attributed to the fact that telecommunications operators have been deploying 4G and 5G technologies. Cybercriminals have taken advantage of the fastness of these technologies.

The digital transactions solutions specialist indicated that the IoT and sensors make it easy for cyberattacks. She went further and said that:

> Because billions of devices and things are connected through the internet network, it is easy for cyber-fraudsters to target and attack a specific system.

While most people and organisations are implementing and enjoying the benefits of 4IR technologies and the speed of 5G, they are not fortifying their cybersecurity. In March 2022, the Independent Communications Authority of South Africa auctioned a high-demand radio frequency spectrum (Dagada 2022b). There were six successful bidders, namely, Vodacom, Rain, MTN, Liquid Intelligent Technologies, and Cell C. The executive director of infrastructure gave the following explanation:

> Before the allocation of the high-demand spectrum, it was a very expensive and tedious process for the local mobile operators to deploy 4G and 5G technologies. Now it has become cheaper, easier and quicker to roll out these technologies. Most operators are only focusing on the deployment of 5G. Cybercriminals have been using this technology to attack information systems and data centres.

The 4IR and 5G have led to the increasing convergence of technologies, as the investment specialist concurred:

> While convergence of technologies comes with massive advantages for individuals, households, and businesses, it presents huge cybersecurity challenges. Of course, this can be mitigated by tightening one's cybersecurity. Cybersecurity practitioners and companies should "up their game" to tackle the "scourge of increasing cybercrime in the country.

An impression should not be created which suggests that companies are not serious regarding their cybersecurity responsibilities. The head of risk management asserted that:

> Some of the companies that have been cyberattacked in South Africa are in the financial services sector and listed in stock exchanges. There is no way they would adopt a lackadaisical attitude towards the protection of their ICT infrastructure and system.

It seems cybersecurity companies and professionals have been "caught napping" by cybercriminals and the "unprecedented convergence" of technologies. This explains why the International Cyber Exposure Index has been ranking South Africa sixth on the list of most targeted countries for cyberattacks during the past six years.

5G technology has drastically upscaled the latency between devices. Latency is the time that it takes for the signal to move from the source to the targeted destination and return to the source. The head of virtual channels highlighted that:

> The lighting speed of latency is a gift to cyberfraudsters to deploy ransomware. That's why you have been seeing a rapid increase in cybercrime.

The advanced latency is very essential for the efficiency of computation, biotechnology, quantum technologies, augmented and virtual reality, the metaverse, AI, flying cars, advanced robotics, drones, and other driverless cars (Dagada 2021). Unfortunately, these developments bring with them increasing cyberattacks.

Covid-19 has increased the trend of working and studying from home, as the risk analyst explained:

> This is enabling cybercriminals to target critical organisational information in less cyber-secured environments like homes. Unfortunately, this kind of attack won't just affect an isolated individual in their home, but the whole organisation will be affected.

When employers provide their employees with the tools to work from home, necessary measures should be taken to protect the organisation's information systems.

Cybercriminals are making use of generative apps, such as ChatGPT, Bard and Bing Chat, to defraud unsuspecting users. These apps are highly driven by AI, big data, and the IoT. The most popular among them is ChatGPT. It reached 1 million users much quicker than Facebook, Instagram, Twitter, Pinterest, and other social media apps. The team leader for applications development indicated that:

> ChatGPT is used by criminals to create convincing phishing messages that would trick users into downloading malware or provide sensitive information such as banking details. Cyberfraudsters use ChatGPT and similar apps to create a convincing digital copy of someone who is your business or professional associate to defraud you through this kind of impersonation.

Criminals use apps, such as ChatGPT, Bard and Bing Chat, to generate various types of scamming materials that look genuine and convincing, including fake emails, listings and advertisements. This enables the ChatGPT to automate the compositing of phishing and malicious emails that are used by cybercriminals to embark on large-scale attacks much more easily.

The Government and Corporate South Africa Are Largely Inadequately Equipped to Deal with Cyberattacks

In 2002, the then Director General of the National Intelligence Agency (NIA), Vusi Mavimbela, stunned security experts when he revealed that most companies in South Africa are victims of the cybercrime of industrial espionage. Industrial espionage is commercial spying and unlawful acquisition of business information and critical technologies for competitive advantage. Since 2005, I have been immersed in the study of cybercrime and found that by 2022, industrial espionage was still rampant in South

Africa. This should be attributed to four factors that were revealed during the fieldwork for the current study.

Firstly, corporate South Africa is largely very naïve when it comes to cybercrime. The chief security advisor declared that:

> Except for the banks, most South African companies have done very little to mitigate industrial espionage which is mostly conducted through hacking and social engineering.

Even when they are alerted that they are being spied on, they usually fail to take the warning seriously.

Secondly, corporate South Africa lacks cybersecurity experts and thus they outsource this service to foreign companies. In some instances, these foreign companies that masquerade as private security firms are intelligence operatives that siphon the intellectual property of corporate South Africa to their competitors in their home countries. This intellectual property includes sensitive commercial data, trade secrets, and new technology invented by South African companies valued at billions of rands. The cybersecurity analyst was very critical of some of the South African government's actions that discourage foreign investment. He was sympathetic to the African National Congress' suspicion of foreign security companies:

> Most countries will be very hesitant to have many foreign security companies operating within their borders.

Thirdly, although the State Security Agency (SSA) is aware that corporate South Africa is a victim of industrial espionage, the truth is that all the government security agencies lack the technical expertise to combat cybercrime. The irony is that the country has one of the most highly acclaimed commercial laws in the world, that is, the ECT Act. The lawyer explained that:

> One of the provisions of the ECT Act is that the government should appoint cyber inspectors [colloquially called "cybercops"]. More than 20 years after the promulgation of this law, the South African Police and intelligence services do not have the manpower and capacity to tackle cybercrime and industrial espionage. Most police and intelligence officers don't have basic skills and access to the internet.

Fourthly, there has been disregard of the cybersecurity-related laws and the King III Report on Corporate Governance by most South African companies. The professor of commercial law noted the following:

> It appears they don't seem to be aware that failure to comply with the provisions of the law renders their commercial websites and apps to huge risks.

Of the 1 550 websites assessed by Buys Incorporated Attorneys in 2004, the Telkom website was the only one to score a full 100% compliance rate (Dagada 2021). The state of website compliance has not improved to date; the current study found that most South African companies have negative attitudes towards cybersecurity legislation.

The above-mentioned four factors have led to the unabated growth of industrial espionage in South Africa. The rapidly increasing industrial espionage cannot be allowed to continue unmitigated. Business associations and professional bodies should devise programmes to educate their members regarding industrial espionage. There should be public-private partnerships to deal with this scourge. The government should appoint some of the best graduates to intelligence services and pay them well. The adjunct professor reasoned as follows:

> The practice of mainly employing people who could not make it to other professions due to poor academic performance into the police and intelligence services should be stopped. How can we place the security of the state and companies' intellectual property in the hands of the officers who were not bright at school?

Corporate South Africa and universities should work together to grow their timber in terms of security expertise instead of relying on foreign specialists. If South Africa wants to thrive in the highly competitive globalised and commercial world, these are some of the things it should consider in protecting its intellectual property. The general manager for regulatory affairs said that:

> It is surprising that in this day and age, politicians and journalists still get excited about reports related to spying activities. The truth is most countries spy on each other. The main purpose of an embassy is not just merely to strengthen relations between two countries or to issue visas, but rather to collect strategic political and trade information from the host country.

In other words, countries that have embassies in each other are conducting intelligence and counterintelligence on each other. Of course, this is wrong – but the reality is that it is happening, and South Africa should equip itself sufficiently to protect its intellectual property, technologies, and trade secrets. The portfolio manager asserted that:

> Spying is not confined at sovereign level; major companies also spy on each other, and this is commonly called "industrial espionage".

Industrial espionage is the least-known concept within the intelligence compendium although many agencies are now involved in this activity. France, the US, China and Israel now have intelligence units responsible for collecting and coordinating industrial intelligence (Dagada 2021). Several private businesses have been mentioned in cases involving the illegal theft of commercial information. The head of portfolio highlighted the following:

> This attests to the fact that in modern societies, as was the case in earlier centuries, economic intelligence is an integral aspect of business, albeit as a business risk.

The study has found that industrial espionage in South Africa is on the rise. A variety of covert and overt instruments exist to enable competitors to acquire business information to increase their competitive advantage. South Africa's businesses do not have adequate security fortitude in place to protect themselves; this includes the state-owned entities. The head of enterprise information architecture declared that:

> Industrial espionage is easily succeeding with the aid of 4IR technologies and where there are no proper security measures to prevent the stealing of business information.

The widespread presence of industrial espionage in South Africa could be an indicator that domestic corporate security frameworks have so far failed to neutralise the industrial espionage threat. An analysis of the study showed that industrial espionage is one of the major risks of business operations. Business rivals apply several instruments, including human and technical sources of intelligence, which are believed to be the most preferred means of perpetuating this criminal activity.

Intelligence refers to information that has been collected and analysed about a target, as the adjunct professor explained:

> This information is assembled through overt and covert methods, including collection from grey sources, which are diplomatic and overt government documents. Industrial espionage entails the purposeful gathering of information of economic and business value related to trade secrets, product formulae, concealed business strategies, trade negotiation strategies, business plans, and product development of industry competitors.

Industrial espionage is not restricted to collection from open sources; the gathering of concealed strategic business secrets is also highly prized. This activity is, nonetheless, carried out by both private entities and government security agencies.

Global integration of ICT and advancement of 4IR technologies are fuelling the exponential growth of industrial espionage. Previously disparate societies have integrated through globalization and the network knowledge economy. The senior researcher asserted that:

> The combination of globalisation and the growth of 4IR has led to a huge surge in industrial information crime.

From its humble beginnings in the 1950s, internet technology has developed exponentially. Its ability to link people, organisations and businesses is the major advantage for the commission of industrial espionage. This connectivity enables hackers and other cybercriminals to carry out their operations with ease. The head of virtual channels indicated that:

> The same technology allows for stolen information to be easily concealed from de jure authorities and illegally transmitted to clients.

The conclusion is that the rise of the 4IR in a globalised environment has seen a concomitant rise in the rate and spread of industrial espionage. Ineffective counterintelligence measures are also responsible for the growth of industrial espionage. The chief risk officer made the following observation:

> Most business enterprises do not seem to be conscious of the importance of having high quality security measures in place. They continue to use old and outdated security management infrastructure that solely prioritises physical security whilst oblivious to the need to protect information in accordance with modern techniques.

Physical security-based approaches to cybersecurity are often rudimentary and inadequate. Competent anti-espionage security systems should, amongst others, target ICT infrastructure, ICT end-user security awareness, and electronic recording and information transmission devices.

The government's tardiness in implementing cybersecurity legislation impacts the business sector's attitude towards legislation. It was revealed that the attitude of corporate South Africa towards the implementation of the requirements of cybersecurity laws is partly affected by the way the government performs its responsibilities towards the implementation and improvement of the legislation. Certain provisions in the ECT Act had not yet been implemented by the time of writing this article, even though the legislation was promulgated back in 2002. Amongst others, this pertains to the appointment of the cybercops.

The head of digital banking in one of the four largest South African banks argued that cybercops in South Africa are largely found in the banks and few other organisations:

> South African banks have dedicated teams of cybersecurity professionals who "combat" internet-related crimes. After noticing clients' concerns regarding digital banking crime, banks respond forcefully, and with superiority, to prevent financial losses and reputational damage.

Cybercops in the banking industry remove phishing and spoofing websites swiftly whilst suspicious emails are blocked before they reach the targeted victim. This observation was supported by the managing executive of digital banking channels of another big bank:

> We ensure that we have got monitoring systems, behaviour pattern analysis, and early warning systems. For example, if a spoofing site is picked up worldwide on the Internet or a phishing email goes out, we typically shut the site down within 45 minutes to two hours. It doesn't matter where it sits in the world.

Banks are also available 24 hours a day to help their customers in cases where they suspect their digital banking accounts are being defrauded. Customers can phone the contact centre, "and there is also a button on the banking website or app that says, 'Do you want to report a fraud incident', press the button – they will close your digital banking facility immediately".

The head of virtual channels in one of the banks asserted that there are times when cybercops in South Africa prevent money from leaving bank accounts fraudulently. They also ensure that transactions via digital banking are undertaken in an encrypted environment. Criminals cannot intercept encrypted transactions. It was also found that banks were more compliant with regard to the cybersecurity aspects of the legislation than all other industrial sectors in South Africa.

A researcher attached to a security institute argued that South African banks had no choice but to comply with the legal aspects of cybersecurity:

> They are however motivated by business considerations rather than solely being loyal to what the legislation prescribes. Companies in other industrial sectors don't have huge volumes of transactions across cyberspace like the banking sector. Consequently, they have very little interest in establishing organs like SABRIC or establishing their sophisticated teams to fight cybercrimes.

The head of enterprise information architecture at a hotel group concurred:

> We work with the government through the Business Against Crime initiative, but the government should take leadership when it comes to cybersecurity crimes, otherwise companies in South African will end up operating paramilitary entities and that is not good in a constitutional state; I mean we are not in the business of securing the country; we are hoteliers. You can argue that the government is breaking the law by delaying the implementation of certain aspects of the Electronic Communications and Transactions [ECT] Act.

The registration of cell phone SIM cards, as required by law, was done seven years after the promulgation of the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) 70 of 2002.

Cybercriminals are becoming highly sophisticated, and the government should ensure that the legislation is updated and implemented in line with the advancement of 5G and 4IR technologies. The lawyer observed that:

> Corporate South Africa will continue to treat legislation with disdain as long as the government itself does not appear to be carrying out its part of the legal requirements.

It is on this basis that it may be concluded that failure by the government to appear to be taking its own laws seriously has negative ramifications in relation to the attitude of corporate South Africa towards cybersecurity legislation.

Implications of the Study

The study has made practical and theoretical contributions. Firstly, the literature review provided a typology for interlinking 4IR and cybersecurity. This typology can henceforth be used by cybersecurity practitioners to enhance the provision of cybersecurity. A search of scholarly electronic databases and e-journal portals revealed no results pertaining to such a typology. The study findings revealed that there is a correlation between the advancement of 4IR technologies and the rapid increase on cyberattacks. The theory generated in this article revealed the importance of the following: the necessity of ensuring that the executives in corporate South Africa have the appropriate attitude towards cybersecurity-related governance; the role of policymakers and government in providing a regulatory environment that enables organisations to implement cybersecurity properly; the effects of lack of human resources capacity to tackle cyberattacks; and the importance of the applicable pieces of legislation in policy formulation and the implementation of cybersecurity. Thirdly, the originality of the contribution of the study to the scholarly and industry knowledge base of digital transformation benefited from the additional contextualised description which links the advancement of 4IR technologies and rapid increment in cyberattacks in South Africa. Lastly, recommendations that have been made to executives and policymakers constitute the practical contribution of this study. Some of the study findings and recommendations may be useful to other countries in Southern Africa and beyond.

Limitations of the Study

Firstly, it was difficult to conduct a study on cybersecurity without somewhat encroaching into the legal field. It was not my intention to interpret the law, but rather to investigate if there was a correlation between the advancement of 4IR technologies and the rapid increase of cyberattacks in South Africa. Since I am not a lawyer, interpretation of the law can be problematic. In some instances, it became very difficult to undertake the aforesaid investigation without providing some legal context and appearing to be interpreting the law. The danger of this action was that there was a very high possibility of my interpreting the law incorrectly. I mitigated this limitation by asking a colleague (a professor of commercial law) to review and provide guidance regarding the legal aspects of the study. Secondly, it was difficult to conduct focus group interviews as part of the qualitative data collection methods in the study. During the proposal stage of the study, it was envisaged that at least two focus group interviews would be conducted. However, the logistics of having participants in groups of at least 12 people became impossible.

Concluding Remarks

Policymakers should ensure that the police, military, and intelligence officers can use advanced technologies to prevent and deal with cyberattacks. That is what governments in China, Russia and West Europe do (Sharikov 2023; Steiger 2022). Unfortunately, the

South African government does not have both skills and infrastructure to do this. The majority of the South African Police Service (SAPS) officers do not even use WhatsApp, emails and the internet. Most of them had never used Facebook, X and other social media apps. Sadly, many of these officers lack basic computing skills (Dagada 2021). Having said that, I should indicate that South Africa used to have highly skilled operatives in the Secret Service (focusing on foreign threats) and the NIA (focusing on domestic threats). Unfortunately, that intelligence capacity was weakened when Jacob Zuma became the president of the country in 2009 (Calland and Sithole 2022). Bright minds were either pushed out of the service or resigned. They were largely replaced by apparatchiks who were largely aligned to political factions.

Zuma amalgamated the NIA, the domestic intelligence service, and the South African Secret Service into the State Security Agency (SSA). However, as was publicly stated at the State Capture Commission, most of the money that was budgeted to fund operations was diverted to fund some factional political activities (Holden 2023). This has largely disadvantaged the SSA from investing in advanced technology infrastructure capable of providing adequate cybersecurity.

The government should work very closely with the private sector to prevent and deal with cyberattacks. Although the government does not have sufficient infrastructure and skilled professionals in government security agencies, they could work with the private sector to do this, and they may not even have to pay a cent. As mentioned in the study findings, according to the ECT Act, the government was supposed to have recruited cybercops; however, seeing that the government is not doing that, the private sector, especially banks, have closed the gap. South Africa's big banks, and a few other companies in other sectors, have employed dedicated teams to fight cybercriminals. The government should upscale its working relationship with SABRIC, Business Against Crime, and private security firms to maximise the use of technology to fight against cybercrime.

Policymakers should be quicker when they embark on the process to make laws. One of the major problems in South Africa is that it is a country of extremes when it comes to regulation. Policymakers, lawmakers and regulators either overregulate or take many years to finalise certain pieces of legislation or regulations (Dagada 2022b). Even after the approval of some brilliant piece of law or set of regulations, the government would, in some instances, take many years to implement the prescripts thereof. Examples of this include the following:

- The provisions of the ECT Act which require the government to employ cybercops have not yet been implemented even though the Act was passed in 2002. Those who use digital platforms for business purposes remain susceptible to increasing cybercrime while the government is shirking its cybersecurity responsibilities.
- The requirements of RICA to have buyers of mobile prepaid SIM cards registered by mobile network operators so that the law enforcement agencies can identify them

if their mobile numbers are used in the execution of criminal activities were only implemented in 2009 even though this law was promulgated in 2002. This has left the sellers and buyers in digital business environment vulnerable to cybercrime.

- The PoPI Bill was introduced way back in 2009, but it was only signed into law as the PoPI Act in 2013. It is important to note that the PoPI Act is an enforcement law rather than a guiding legislation. However, some of the provisions of this legislation had not yet been put into effect on 1 July 2021 (these include sections 110 and 114(4).

I think that some provisions in several regulations and the implementation of some prescripts in various pieces of legislation will never materialise. South African policymakers should be commended for crafting the Cybercrime Bill. In 2021, President Ramaphosa signed it into law, the Cybercrimes Act 19 of 2020. The reason why cybercriminals have been moving their activities to emerging economies in general and South Africa is because most of these jurisdictions do not have laws to deter and prosecute cybercrime. The inception of the Cybercrimes Act was a significant step towards tackling cybercriminals and aligning the country with developed economies which should boost their confidence in digital business in South Africa.

References

Brynjolfson, E., and A. McFee. 2014. *Second Machine Age: Work, Progress and Prosperity in a Time of Brilliant Technologies*. New York: W.W. Norton.

Calland, R., and M. Sithole. 2022. *The Presidents: From Mandela to Ramaphosa, Leadership in the Age of Crisis*. Cape Town: Penguin Books.

Campbell, D. 2005. *E-Commerce and the Law of Digital*. London: Oxford University Press.

Chaka, C. 2023. "Fourth Industrial Revolution: A Review of Applications, Prospects, and Challenges for Artificial Intelligence, Robotics and Blockchain in Higher Education." *Research and Practice in Technology Enhanced Learning* 18 (2): 1–39. https://doi.org/10.58459/rptel.2023.18002

Corallo, A., M. Lazoi, M. Lezzi, and A. Luperto. 2022. "Cybersecurity Awareness in the Context of Industrial Internet of Things: A Systematic Literature Review." *Computers in Industry* 137 (4): 1–16. https://doi.org/10.1016/j.compind.2022.103614

Crume, J. 2000. *Inside Internet Security: What Hackers Don't Want You to Know*. New York: Addison-Wesley.

Dagada, R. 2013. "Digital Banking Security, Risk and Credibility Concerns in South Africa." Paper presented at the Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013), Kuala Lumpur, 4–6 March.

Dagada, R. 2021. *Digital Business Governance in the Era of Fourth Industrial Revolution in South Africa*. Pretoria: Unisa Press.

Dagada, R. 2022a. "The Luddites Are Back: But Both Technology and Humans Shall Prevail." In *Research in Southern African Digital Business,* edited by G. J. Lee and R. Dagada, 269–290. Johannesburg: Silk Route Press.

Dagada, R. 2022b. "A Chequered Journey en route to Digital Business: Lessons from the South African Banking Sector." In *Research in Southern African Digital Business,* edited by G. J. Lee and R. Dagada, 291–322. Johannesburg: Silk Route Press.

De Kare-Silver, M. 2001. *E-Shock: The New Rules – Internet Strategies for Retailers and Manufacturers*. New York: Amacom Books.

Diamandis, P. H., and S. Kotler. 2020. *The Future Is Faster Than You Think: How Converging Technologies Are Transforming Business, Industries, and Our Lives*. New York: Simon & Schuster.

Dunlop, A. J. S. 2005. "South Africa." In *E-Commerce and the Law of Digital Signatures,* edited by D. Campbell, 559–578. London: Oxford University Press.

Fang, Y., and I. Qureshi. 2014. "Trust, Satisfaction, and Online Repurchase Intention: The Moderating Role of Perceived Effectiveness of E-Commerce Institutional Mechanisms." *MIS Quarterly* 38 (2): 407–438. https://doi.org/10.25300/MISQ/2014/38.2.04

Fourie, J. 2021. *Our Long Walk to Economic Freedom: Lessons from 100 000 Years of Human History*. Cape Town: Tafelberg. https://doi.org/10.1017/9781009228503

Gavaza, M. 2020. "South Africa Number Three on World List of Most Cybercrime Victims." *BusinessDay*, May 29. https://www.businesslive.co.za/bd/companies/telecoms-and-technology/2020-05-29-sa-number-three-on-world-list-of-most-cybercrime-victims/

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

Ghimire, B., and D. B. Rawat. 2022. "Recent Advances on Federated Learning for Cybersecurity for Federated Learning for Internet of Things." *IEEE Internet of Things Journal* 9 (11): 8229–8249. https://doi.org/10.1109/JIOT.2022.3150363

Greenhalgh, T., and R. Taylor. 1997. "Papers That Go Beyond Numbers (Qualitative Research)." *British Medical Journal* 315 (7110): 740–743. https://doi.org/10.1136/bmj.315.7110.740

Holden, P. 2023. *Zondo at Your Fingertips*. Johannesburg: Jacana.

Jackis, K., and S. M. Abass. 2019. "Developing History of the World Wide Web." *International Journal of Scientific and Technology Research 8* (9): 75–79.

Kenny, N., A. Doyle, and F. Horgan. 2023. “Transformative Inclusion: Differentiating Qualitative Research Methods to Support Participation for Individuals with Complex Communication or Cognitive Profiles.” *International Journal of Qualitative Methods* 22 (5): 1–17. https://doi.org/10.1177/16094069221146992

Li, Y., and S. Zhang. 2022. “Qualitative Data Analysis.” In *Applied Research Methods in Urban and Regional Planning*, edited by Y. Li and S. Zhang, 149–165. Cham: Springer. https://doi.org/10.1007/978-3-030-93574-0_8

Mabunda, S. 2021. “Cybersecurity in South Africa: Towards Best Practices.” In *CyberBRICS Countries*, edited by L. Belli, 227–270. Cham: Springer. https://doi.org/10.1007/978-3-030-56405-6_6

Maiwald, E. 2004. *Fundamentals of Network Security*. New York: McGraw-Hill Technology Education.

Merriam, B. S. 1998. *Qualitative Research and Case Study Applications in Education*. San Francisco: Jossey-Bass.

Mijwil, M., O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani. 2023. “Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview.” *Mesopotamian Journal of Cybersecurity*, 57–63. https://doi.org/10.58496/MJCS/2023/010

Netshakhuma, N. S. 2023. “Cybersecurity Management in South Africa Universities.” In *Cybersecurity Issues, Challenges, and Solutions in the Business World*, edited by N. S. Netshakhuma, 196–211. Hershey: IGI Global. https://doi.org/10.4018/978-1-6684-5827-3.ch013

Othman, K. 2022. “Exploring the Implications of Autonomous Vehicles: A Comprehensive Review.” *Innovative Infrastructure Solutions* 7 (2): a165. https://doi.org/10.1007/s41062-022-00763-6

Paulus, T. M. 2023. “Using Qualitative Data Analysis Software to Support Digital Research Workflows.” *Human Resources Development Review* 22 (1): 139–148. https://doi.org/10.1177/15344843221138381

Saura, J. R., D. Palacios-Marques, and B. Barbosa. 2023. “A Review of Digital Family Businesses: Setting Marketing Strategies, Business Models and Technology Applications.” *International Journal of Entrepreneurial Behaviour and Research* 29 (1): 144–165. https://doi.org/10.1108/IJEBR-03-2022-0228

Schoonenboom, J. 2023. “The Fundamental Difference between Qualitative and Quantitative Data in Mixed Methods Research.” *Forum: Qualitative Social Research* 24 (1): a11.

Schwab, K. 2017. *The Fourth Industrial Revolution*. London: Penguin Books.

Sharikov, P. 2023. “Contemporary Cybersecurity Challenges.” In *The Implications of Emerging Technologies in the Euro-Atlantic Space*, edited by J. Berghofer, A. Futter, C. Häusler, M. Hoell and J. Nosál, 143–157. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-24673-9_9

Shrivastava, S. R., and P. S. Shrivastava. 2023. “Data Collection Process in Qualitative Research: Challenges and Potential Solutions.” *Medical Journal of Dr DY Patil University* 16 (3): 443–445. https://doi.org/10.4103/mjdrdypu.mjdrdypu_871_21

Steiger, S. 2022. “Cyber Securities and Cyber Security Politics.” In *Cyber Security Politics*, edited by M. Dunn Cavelty and A. Wenger, 141–153. London: Routledge. https://doi.org/10.4324/9781003110224

Sutherland, E. 2017. “Governance of Cybersecurity: The Case of South Africa.” *African Journal of Information and Communication* 20: 83–112. https://doi.org/10.23962/10539/23574

Truman, S. E. 2023. “Undisciplined: Research-Creation and What It May Offer (Traditional) Qualitative Research Methods.” *Qualitative Inquiry* 29 (1): 95–104. https://doi.org/10.1177/10778004221098380