National Critical Information Infrastructure Protection Through Cybersecurity: A National Government Perspective

Thuli Mkhwanazi and Lynn Futcher
Nelson Mandela University, Summerstrand, South Africa
Council of Scientific and Industrial Research (CSIR)

S216316987@mandela.ac.za
lynn.futcher@mandela.ac.za

Abstract: The South African national government is forging ahead with digitalisation plans to enhance socioeconomic growth in the country. However, digitalisation is accompanied by detrimental cybersecurity risks that may potentially exacerbate the vulnerability of the National Critical Information Infrastructure (NCII) of South Africa to cyber-attacks. Therefore, the envisaged digitalisation benefits in South Africa may be offset by the increased cybersecurity risk on the NCII of the country.

Through a theoretical literature review, this study aims to investigate digitalisation and identify the cybersecurity risks it poses to the National Critical Information Infrastructure of South Africa, from a national government policy perspective. A gap has been identified in Information and Communications Technology for Development (ICT4D) research studies that researchers tend to focus on the implementation of ICTs while neglecting the policy aspect that is meant to direct and control the implementation of ICTs. Therefore, this study bridges this gap by approaching digitalisation and cybersecurity from a national government policy perspective. The output of this study is a National Critical Information Infrastructure Protection (through Cybersecurity) Conceptual Framework (NCIIP-CF) that is applicable to all spheres of government (local, provincial or national) as policy makers. The NCIIP-CF demonstrates an approach that embeds cybersecurity in the digitalisation process for the national government of South Africa, thus enabling an NCII that is resilient to cybersecurity risks.

Keywords: Digitalisation, Fourth Industrial Revolution, Cybersecurity, South African Government, National Cybersecurity, National Critical Information Infrastructure

1. Introduction

Digitalisation, also known as the "Fourth Industrial Revolution" or "Industry 4.0," is a global megatrend (Department of Science and Technology, 2019; Thun et al., 2019) that has that gained attention from influential international countries and organisations, like the World Economic Forum (WEF) (Cunningham, 2018), Group of 20 (G20 Osaka Leaders, 2020), and Brazil, Russia, India, China and South Africa bloc (BRICS Heads of State and Government, 2018). It aims to amplify socioeconomic productivity through the diffusion of emerging technologies (Bican and Brem, 2020). The COVID-19 pandemic accelerated the global transition to digitalisation, leading to the South African government prioritizing digitalisation plans (Schwab, 2020; Wang et al., 2019).

However, digitalisation presents cybersecurity risks, particularly on the National Critical Information Infrastructure (NCII) (Abdullah et al., 2019; Cunningham, 2018; Laufs et al., 2020; Victoria, 2019). National governments are responsible for protecting the NCII through cybersecurity measures. However, the South African government has not fulfilled this mandate successfully, with several cyber-attacks causing significant economic loss (Griffiths, 2017; Sutherland, 2017; Van Niekerk, 2017).

This paper proposes an NCII Protection Conceptual Framework (NCIIP-CF) to mitigate these risks, prioritizing national cybersecurity in the digitalisation process from the beginning, which is the public policy planning phase.

This paper outlines the structure of digitalisation and its critical components (Section 2), the NCII (Section 3), NCII protection through cybersecurity (Section 4), and a conclusion (Section 5).

2. Digitalisation

Digitalisation is the process of transforming world systems (social, economic and political) into a borderless domain, through digitisation. Digitisation is the technological process of transforming physical or manual systems, services or products from a static format to an interactive and autonomous one that can be stored, processed and transmitted electronically using extensive computational power (Bican and Brem, 2020). Table 1 presents some of the emerging technologies being referred to when speaking of digitisation (Bican and Brem, 2020; Pillay et al., 2016; Victoria, 2019). Digitisation combines interdependent physical, digital and biological elements into novel products and services (Schwab, 2016).

Table 1: Digitisation Emerging Technologies (Bican and Brem, 2020; Cunningham, 2018; Mitchell, 2020; Schwab, 2016)

Physical emerging technologies	Digital emerging technologies	Biological emerging technologies
3D Printing	IoT	Genetic sequencing
Autonomous vehicles	AI	Gene edition or activation
New material	Blockchain	Synthetic biological cells
Robotics	Virtual and augmented reality	Neurotechnology
Quantum computers	5G	
Space technologies	Social media	
	Cloud technology	

Widespread digitisation will, in turn, transform the entire structure of interaction between humans and the world systems, which is a phenomenon known as digitalisation.

2.1 Digitalisation Theoretical Framework

Digitalisation is not rooted in Information and Communication Technologies (ICT) as common sense would argue, but rather in historic economic cycles (Hilbert, 2012). Conceptually, economic cycles are wave-like occurrences, where the incline represents the rising innovation which increases industrial productivity, profits and economic growth until a point of equilibrium is reached (Perez, 1985; Schumpeter, 1939). The point of equilibrium occurs when the innovation has served its purpose and ceases to be novel; thus, leading to a decline in industrial productivity, profits and economic growth, moving into a recession phase (Schumpeter, 1939). A recession phase calls for innovation and thus for another economic cycle (Perez, 1985; Schumpeter, 1939). There are various economic cycles, including 'Kondratieffs, Kitchins and Juglars' (Schumpeter, 1939, p. 176). Schumpeter deduced that, of the above-mentioned three economic cycles, the Kondratieff is an industrial revolution (IR) (Schumpeter, 1939). An IR is a group of related and interdependent innovations that, when largely adopted in industry, bring about a transformation in the broader social and economic structures of a nation (Schumpeter, 1939). Schumpeter's description of an IR fits the description of digitalisation. Hence this study regards the fourth IR (4IR) as the theoretical framework of digitalisation.

The next section discusses ICT for Development (ICT4D) as a conceptual framework for digitalisation.

2.2 Digitalisation Conceptual Framework

From a high-level overview of digitalisation, the themes of emerging digital ICT and socioeconomic development can be deduced. This is drawn from the concept of ICT4D (Ordóñez, 2015). ICT4D entails projects that are conducted by donors to establish or to improve the state of ICT systems of recipients, for socioeconomic development (Chipidza and Leidner, 2019). Depending on the locale of the ICT4D project, the donors are the initiators of the ICT4D project as they are more capable of doing so owing to the availability of resources to them (Hilbert, 2012). Typically, donors are international influencers who are superior in terms of socioeconomic development (Kunyenje, 2019). Therefore, the likes of BRICS, G20, WEF, and United Nations (UN), referred to in Section 1 represent donors taking up the role of assisting the recipients. Donors are not limited to influential countries — they could be researchers, governing authorities, private banks or any stakeholder taking up the role of assisting the recipients (Chipidza and Leidner, 2019; Hilbert, 2012). The recipients are the beneficiaries or subjects who will supposedly benefit from the ICT4D project, be it a government, public sector, community or typically, a developing country like South Africa (SA) (Chipidza and Leidner, 2019; Schia, 2018). As such, digitalisation qualifies to be viewed through the lens of ICT4D in developing countries since it comprises the harnessing of emerging digital ICT for socioeconomic development, and it is promoted by donors.

Figure 1 presents the ICT4D-CF that was originally established by the United Nation's Economic Commission for Latin America and the Caribbean (UN-ECLAC) and modified by Hilbert in 2012 (Hilbert, 2012).

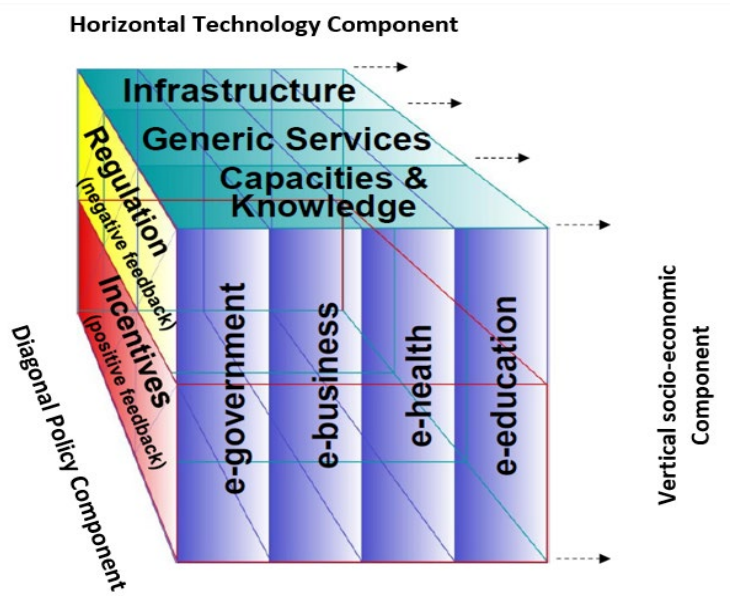

Figure 1: Modified Version of the ICT4D Cube (Hilbert, 2012)

The ICT4D-CF was developed to use as a guide for international, national and local governments, when conducting the policy process towards transitioning into an information society (Hilbert, 2012). This transition is referred to as digitalisation in this study. The three critical components of the ICT4D-CF as depicted in Figure 1 are as follows (Hilbert, 2012):

- The **Horizontal Technology Component** represents the fundamental ICT infrastructure that enables digitalisation. The ICT infrastructure includes computer software, hardware, networks and communication protocols. In computer science the ICT infrastructure is categorised in terms of the Open System Interconnection (OSI) Reference Model, which includes physical ICT and digital generic ICT services. Human skills are required to develop and implement the ICT infrastructure thus making the capacities and knowledge layer.
- The **Vertical Socio-economic Component** represents the various socioeconomic sectors to be digitalised, which are not limited e-government, e-business, e-health and e-education as shown in Figure 1.
- The **Diagonal Policy Component** represents the policy process, legislation and regulation frameworks that are supposed to promote, direct and control digitalisation.

It is the policy process (Diagonal Component in Figure 1) that plays a crucial role in digitalisation (World Economic Forum, 2020). A policy process generally involves a number of stages or cycles, from identifying policy problems and objectives, to executing, monitoring and evaluating those policy objectives (Kunyenje, 2019). The public policy process may be categorised into three broad stages of planning, execution, and evaluation (Hilbert, 2012).

The focus of this paper is on the planning stage of the governmental policy process. Government policies are crucial determinants of national socioeconomic development, hence the approach of digitalisation from a government's policy perspective. The ICT4D-CF is a useful tool in providing an overview of the critical components at play throughout the digitalisation policy process. Digitalisation is conceptualised by this paper through the ICT4D-CF in Figure 1. Ultimately, digitalisation transforms the national critical infrastructures (NCI) into NCII.

3. The National Critical Information Infrastructure

This section discusses the evolution of socioeconomic sectors from being NCI to becoming an interconnected NCII through digitalisation. An NCI transforms into an NCII once its innovations are dependent on ICT, specifically information/data and the internet. In SA, NCII is defined as:

> *"all ICT systems, data systems, databases, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the Republic … This relates to critical services such as the economy, social services and law enforcement (inclusive of the justice system and state security)" (State Security Agency, 2015).*

From the above definition of NCII, three themes can be observed, namely: (1) the extension of ICT systems, (2) to operate national systems, (3) for socio-economic benefits. Therefore, this paper defines digitalisation as the digitisation of the National Critical Infrastructure (NCI) into an NCII resulting from the diffusion of emerging technologies across socioeconomic and political sectors. NCII describes an internet-connected strategic unit that provides essential services to the nation for the purpose of socioeconomic and political development and resilience (Runciman, 2006), through the harnessing of ICT. Twelve CIs are declared as NCII in SA and are listed, in no particular order, in Table 2.

Table 2: South African National Critical Information Infrastructure (Pillay, 2017)

Critical Infrastructures		
Manufacturing	Electricity/Energy	Police, defence and legal
Emergency services	Financial services	Telecommunications
Health services	Information Technology	Transportation and ports
Key government agencies	Liquid fuels	Water/Sanitation

On the ICT4D-CF in Figure 1, the socioeconomic sectors representing the CIs in Table 2 are prefixed with an 'e' to indicate their methods of productivity as being reliant on the internet (Hilbert, 2012). The implication of e-health or e-government, for example, is that the public may interact with computer applications through the sharing of information over the internet to access essential public services, instead of through physical interaction.

The next section presents the NCII Conceptual Framework (NCII-CF).

3.1 National Critical Information Infrastructure Conceptual Framework

Interconnectedly, Critical Infrastructures (CI) and the Critical Information Infrastructure (CII) make up the NCII. The NCII-CF is informed by a literature review and the ICT4D-CF in Figure 1. The NCII-CF, like the ICT4D-CF, consists of three critical components of technology (i.e., CII), socio-economic sectors (i.e., CI) and policy (i.e., Regulatory Framework).

CII describes an ICT infrastructure consisting of interconnected hardware, software, networking devices, equipment and services — these include computer devices, applications, operating systems, the internet and its services, and all other tangible and intangible ICT tools (Christensen et al., 2010; Hilbert, 2012; State Security Agency, 2015). These are the systems and tools that are shared within and across the various NCIs to carry out operational business activities (Runciman, 2006). As such, the emerging technologies in Table 1 are regarded as CII. Since human beings possess information in the form of intelligence and skills, they are essential in developing and operating ICT systems. As such, human beings are regarded as human capital. In the ICT4D-CF in Figure 1, human "capacities and knowledge" are similarly positioned in the horizontal technology component (Hilbert, 2012).

CIs refer to physical buildings or locations (Christensen et al., 2010) of the socioeconomic entities that are declared as NCII (see Table 2). CIs are the socioeconomic entities or organisations whose services are essential for civil development, national wealth, and national security (Sofaer et al., 2010). CIs depend on the CII for their operations, represented by the vertical socio-economic sectors component (see Figure 1).

Distinguishing between CI and CII made more sense in the previous IRs or prior to digitalisation where clear physical and digital boundaries existed. In contrast, digitalisation is essentially concerned with diminishing those boundaries, evidenced by its applications combining physical, biological and digital technologies into innovative products and services. Figure 2 presents the NCII-CF which is adapted from the ICT4D-CF in Figure 1.

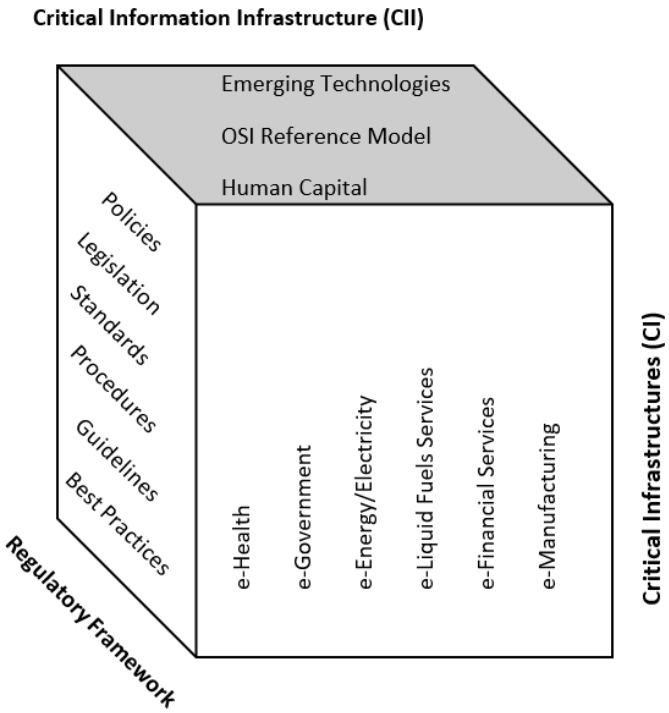

Figure 2: National Critical Information Infrastructure Conceptual Framework (adapted from Hilbert (2012))

Digitalisation implies an NCII whose production and productivity depend on emerging technologies, high interconnectivity (OSI Reference Model) and a digitally skilful workforce. Furthermore, digitalisation implies that the NCII is a borderless domain that exists and operates in cyberspace. The dependence on cyberspace of the NCII introduces significant cybersecurity concerns to governments worldwide (Kortjan, 2013; State Security Agency, 2015). This is due to the prevalence of cyberattacks on NCII (Griffiths, 2017; Pillay, 2017).

3.2 Cyberattacks on the National Critical Information Infrastructure

NCII attacks can either target CIs and thus be limited to physical damage (Christensen et al., 2010), or they can target the CII, which can result in the loss of confidentiality, integrity or availability (CIA) of the CII (State Security Agency, 2015). Digital attacks against NCII are known as cyberattacks.

According to the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 2700:2009), an attack is "*an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset*" (ISO/IEC, 2012, p. 3). If an attack and assets are in cyberspace, it is then a cyberattack. The NCII is the most targeted asset in cyberspace (Gkioulos and Chowdhury, 2021). Typical cyberattacks against NCII are cybercrime, cyberespionage, cyberterrorism, cyberwarfare or information warfare, denial of service (DoS), distributed denial of service (DDoS) and hacktivism, which are all meant to disrupt the CIA of the NCII (Christensen et al., 2010; Griffiths, 2017; Runciman, 2006; Yunos et al., 2015). The above-mentioned cyberattacks may be categorised into cyberterrorism, cyberespionage, cyberwarfare and cybercrime (Griffiths, 2017). These four categories of cyberattacks are what the Ministry of Defence Estonia (2008), and State Security Agency (2015) SA noted as new and sophisticated cyberthreats to NCII resulting from digitalisation (Ministry of Defence Estonia, 2008; State Security Agency, 2015). While cyberattacks may occur at an individual, organisational or state level, cyberattacks on the NCII are the most detrimentally impactful of all cyberattacks (Ministry of Defence Estonia, 2008).

Pillay (2017, p. 9) adds "state-to-state conflict" as a form of cyberterrorism and a cyberthreat to NCII. The assumption therefore is that cyberattacks on NCII are politically motivated and may be carried out by states against other states. This is asserted by similar studies which describe cyberterrorism as politically, socially and economically motivated cyberattacks on NCII, taking place in cyberspace and using offensive cyber tactics which are aimed at harming national government, citizens or the economy (Griffiths, 2017; Yunos et al., 2015).

Figure 3 presents a cyberterrorism conceptual framework that is meant to distinguish the six critical components that establish a cyberattack as an act of cyberterrorism (Yunos et al., 2015). A cyberterrorism conceptual

framework, such as the one in Figure 3, is significant as there are worldwide controversies and disagreements among media, social, political and academic groups concerning attributes that affirm a cyberattack as a cyberterrorism attack.

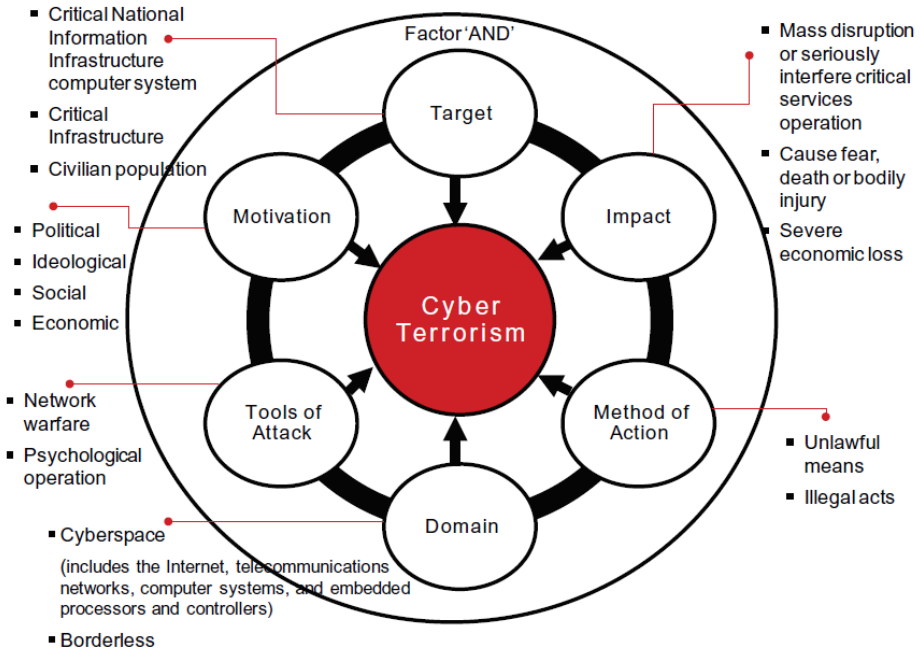

Figure 3: Cyberterrorism Conceptual Framework (Yunos et al., 2015)

Figure 3 conceptualizes six themes related to cyberterrorism concerning typical cyberattacks on NCII. The themes, presented in no particular order, are as follows (Lehto and Neittaanmäki, 2021):

- **Target (1) and Domain (2)**: Identifies components of the NCII-CF vulnerable to cyberattacks, encompassing technologies, processes, and people.
- **Method of Action (3) and Domain and Tools of Attack (4)**: Describes the ways in which the NCII may be attacked, encompassing insiders, ransomware, DDoS attacks, poor encryption, SQL injections, misconfiguration, phishing, trojans, brute force attacks, session hijacking, spoofing, cross-site scripting (XSS), etc.
- **Motivation (5)**: Explores the reasons for cyberattacks on NCII, including "Egoism, Money, Power Paralysis, and Destruction").
- **Impact (6)**: Evaluates the level of disruption that may result from such cyberattacks.

A recent study was conducted to assess the likelihood of state-to-state conflicts arising between SA and the international states it is in strategic partnerships with, which revealed SA as highly vulnerable (Van Niekerk, 2019). SA's cybersecurity approach is noted from the country's cybersecurity legislation, as being only defensive (Van Niekerk, 2019). In fact, South Africa does not have an officially documented national cybersecurity strategy (Phahlamohlaka et al., 2021). Subsequently, it has been asserted that SA has previously been a victim of cyberterrorism attributed to China and Russia. The motive of a state-to-state cyberattack is for a country to gain national power over other countries (van Vuuren et al., 2017). This paper therefore argues that the globally shared agenda of digitalisation may be detrimental to the NCII of SA given the country's vulnerable cybersecurity regulatory framework. It is granted that donors may be beneficial in assisting with the development of cybersecurity in SA (Dewa et al., 2018; G20 Osaka Leaders, 2020; Schia, 2018). However, each country will prioritise its own interests fundamentally (G20 Insights, 2017), even if it means exploiting the national cybersecurity vulnerabilities of an alliance (Griffiths, 2017; Van Niekerk, 2017).

Government has a sovereign responsibility, to ensure a cybersecure NCII as the nation transitions to digitalisation through adequate policy regulatory frameworks.

4. The National Critical Information Infrastructure Protection (Through Cybersecurity) Conceptual Framework

Digitalisation poses indispensable cybersecurity threats to the NCII of SA particularly, as it was emphasised in Section 3.2 that the country is vulnerable, has been previously targeted, and remains susceptible to politically motivated cyberattacks. National government ought to direct the implementation of relevant cybersecurity control measures through the regulatory framework (see Figure 2). Cybersecurity controls are "*means of managing [cybersecurity] risk, including policies, procedures, guidelines, practices …, which can be administrative, technical, management, or legal in nature*" (ISO/IEC, 2012, p. 4).

The South African National Standard 27032:2016 acknowledges that:

> *"… cybersecurity is one of the activities necessary for CIIP, and, at the same time, adequate protection of critical infrastructure services contributes to the basic security needs (i.e., security, reliability and availability of critical infrastructure) for achieving the goals of cybersecurity" (ISO/IEC, 2012, p. 10).*

As such, CIIP is a prioritised and indispensable responsibility of national governments across the globe. This paper suggests that national governments' cybersecurity controls are mainly strategic, such as the public policy process, national cybersecurity strategies, and international cooperation in cybersecurity. Applying the ICT4D-CF (Figure 1) and the NCII-CF (Figure 2), national governments' controls fall within the diagonal *Policy* and the *Regulatory* components, respectively. The diagonal *Policy* component generically represents the strategic controls and policy perspective of digitalisation. This paper has highlighted this component consistently as the most substantial since it directs the technology (horizontal) and socioeconomic development (vertical) components. However, it is important to acknowledge that all three components are interdependent, and none of them is exclusively effective and efficient.

Technical cybersecurity controls describe the implementation of ICT tools, systems and techniques for the purposes of maintaining the CIA of information while it is being transmitted, processed or stored in cyberspace. Applying the ICT4D-CF (Figure 1) and the NCII-CF (Figure 2), this study conceptualises technical cybersecurity controls as falling within the horizontal *Technology* and *CII* components, respectively, to secure the CIA of information assets in the NCII. Technical cybersecurity controls are referred to security domains in the ISO/IEC 27032:2012 and include information security, network security, critical information infrastructure protection (CIIP), internet security, and application security (ISO/IEC, 2012). This study focuses on CIIP which is defined as:

> *"Protecting the systems that are provided or operated by critical infrastructure providers, such as energy, telecommunication, and water departments. Critical Information Infrastructure Protection ensures that those systems and networks are protected and resilient against information security risks, network security risks, Internet security risks, as well as cybersecurity risks" (ISO/IEC, 2012, p. 11).*

The protection of NCII through cybersecurity is a national effort and combination of technical, administrative, legal, regulatory, and strategic security measures, all directed towards socioeconomic development and resilience in the advent of digitalisation. This paper proposes the NCIIP-CF in Figure 3 to conceptualise the protection of NCII through cybersecurity for national governments. The NCIIP-CF is adapted from the ICT4D-CF (Figure 1) and NCII-CF (Figure 2) and also informed by the literature that was reviewed in this study.

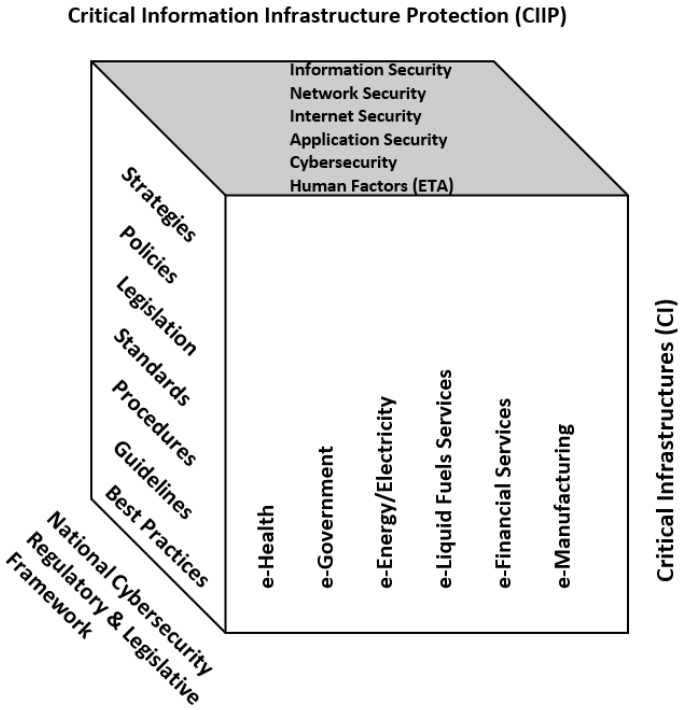

Figure 4: National Critical Information Infrastructure Protection (through Cybersecurity) Conceptual Framework (NCIIP-CF) (adapted from Hilbert (2012))

The NCIIP-CF is a logical and strategic summary and representation of digitalisation, the NCII, and national cybersecurity. It is a three-dimensional cube conceptual framework, which can be used by governments to understand the interdependent functionality of the (i.e., horizontal, vertical and diagonal) components of digitalisation, the NCII and national cybersecurity.

The (horizontal) CIIP component represents the technical cybersecurity controls. In addition to these technical cybersecurity controls are human factors which refer to the cybersecurity skills and awareness of human beings. These technical and human factors cybersecurity controls are necessary to protect each of the elements of CII.

The (vertical) CI component represents private, public and government socioeconomic sectors or organisations that will execute the national cybersecurity regulatory and legislative framework in the diagonal component of the NCIIP-CF. Generically, the vertical component represents the CIs (i.e., sectors, entities or organisations) that are subject to digitalisation.

The (diagonal) national cybersecurity regulatory and legislative framework component constitutes the strategic cybersecurity controls that national governments must lead to control digitalisation planning policy processes. This is the governments' policy perspective of digitalisation, the NCII and cybersecurity. This paper has highlighted this component consistently as the most substantial since it directs the technology (horizontal) and socioeconomic development (vertical) components. All three components of the NCIIP-CF are interdependent.

5. Conclusion

SA is a developing country whose government has aspired to socioeconomic development through the country's public policies and has acknowledged ICT to be the solution. As such, digitalisation plans are well underway in the country. This paper therefore examines digitalisation to understand the phenomenon and to determine the most effective way of implementing it, whilst minimising the cybersecurity risks that it poses.

The critical components of digitalisation include the technology *information infrastructure*, socioeconomic *critical infrastructures* and the strategic *policy* component. The locale or establishment of digitalisation is the NCII which can be categorised into three critical and interdependent components, the CII, CIs and the regulatory framework. The significance of the NCII is that it determines the well-being and survival of a nation. Therefore, disturbance to the functioning of the NCII is highly impactful and should be mitigated, primarily by national government, through national cybersecurity. The NCII of South Africa is particularly vulnerable to politically

motivated cyberattacks. Therefore, digitalisation may expose the NCII of South Africa to politically motivated state-to-state cyber-attacks that are typically committed through cyberterrorism.

As such the NCIIP-CF was proposed to conceptualise digitalisation that prioritises the protection of NCII through government's strategic national cybersecurity controls. The national cybersecurity regulatory and legislative framework component in the proposed NCIIP-CF is meant to ensure cybersecurity in cyberspace, which may result in a society and economy that is developmental, capacitated, proactive and resilient to cyberattacks.

References

Abdullah, T.A.A., Ali, W., Malebary, S., Ahmed, A.A., 2019. A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. IJCSNS International Journal of Computer Science and Network Security 19.

Bican, P.M., Brem, A., 2020. Digital Business Model, Digital Transformation, Digital Entrepreneurship: Is There A Sustainable "Digital"? Sustainability 12, 5239.

BRICS Heads of State and Government, 2018. BRICS in Africa: Collaboration for Inclusive Growth and Shared Prosperity in the 4th Industrial Revolution.

Chipidza, W., Leidner, D., 2019. A review of the ICT-enabled development literature: Towards a power parity theory of ICT4D. Journal of Strategic Information Systems.

Christensen, S., Caelli, W.J., Duncan, W.D., Georgiades, E., 2010. An achilles heel: Denial of service attacks on Australian critical information infrastructures. Information and Communications Technology Law 19, 61–85.

Cunningham, S., 2018. World economic forum and the fourth industrial revolution in South Africa. Trade & Industrial Policy Strategies 30.

Department of Science and Technology, 2019. White paper on science, technology and innovation. Department of Science and Technology 1–70.

Dewa, M.T., Adams, D.Q., Tendayi, T.G., Nyanga, L., Gxamza, M., Ganduri, L., 2018. Industry 4.0: A myth or a reality in South Africa? Proceedings of the 29th South African Institute of Industrial Engineers Conference 575–590.

G20 Insights, 2017. G20 and Africa - Ready for a Steady Partnership ? [WWW Document]. URL www.G20-insights.org (accessed 5.21.20).

G20 Osaka Leaders, 2020. G20 Osaka Leaders' Declaration 1–13.

Gkioulos, V., Chowdhury, N., 2021. Cyber security training for critical infrastructure protection: A literature review. Comput Sci Rev.

Griffiths, J.L., 2017. Cyber security as an emerging challenge to South Africa National Security 88.

Hilbert, M., 2012. Toward a Conceptual Framework for ICT for Development: Lessons Learned from the Cube Framework Used in Latin America (English). Information Technologies & International Development 8, 243–259.

ISO/IEC, 2012. ISO 27032 Information technology - Security techniques - Guidelines for cybersecurity. International Organization for Standardization 50.

Kortjan, N., 2013. A Cyber Security Awareness and Education Framework for South Africa 206.

Kunyenje, G., 2019. Influence of External Actors on National Information and Communications Technology Policy Formulation in Developing Countries: Case of Malawi. University of Cape Town.

Laufs, J., Borrion, H., Bradford, B., 2020. Security and the smart city: A systematic review. Sustain Cities Soc 55.

Lehto, M., Neittaanmäki, P., 2021. Critical Infrastructure Protection Cyber Security. In: Lehto, M., Neittaanmaki, P. (Eds.), Computational Methods in Applied Sciences. Springer Nature Switzerland AG, Cham, pp. 3–36.

Ministry of Defence Estonia, 2008. Cyber Security Strategy Ministry of Defence.

Mitchell, C.J., 2020. The impact of quantum computing on real-world security: A 5G case study. Comput Secur 93, 1–11.

Ordóñez, A., 2015. Impact of Information Society Research in the Global South, A New Set of Questions: ICT4D Research and Policy. Springer Singapore, Singapore.

Perez, C., 1985. Microelectronics, long waves and world structural change: New perspectives for developing countries. World Dev 13, 441–463.

Phahlamohlaka, J., Theron, J., Aschmann, M.J., 2021. National Cybersecurity Implementation in South Africa : The Conundrum Question.

Pillay, K., 2017. National Critical Information Infrastructure Protection Centre. NCIIPC Newsletter 1, 40.

Pillay, K., Ori, A., Merkofer, P., 2016. Industry 4.0: Is Africa ready for digital transformation?, Delloite South Africa.

Runciman, B., 2006. who protects the information our critical infrastructure relies on? [WWW Document]. URL http://0-search.ebscohost.com.wam.seals.ac.za/login.aspx?direct=true&db=bsu&AN=24607744&site=ehost-live&scope=site

Schia, N.N., 2018. The cyber frontier and digital pitfalls in the Global South. Third World Q 39, 821–837.

Schumpeter, J.A., 1939. Business cycles: A theoretical, historical and statistical analysis of the capitalist process, Abridged. ed, McGraw-Hill Book Company. McGraw-Hill Book Company, New York Toronto London.

Schwab, K., 2016. The Fourth Industrial Revolution. World Economic Forum 91–93 route de la Capite CH-1223 Cologny/Geneva Switzerland, Geneva, Switzerland.

Schwab, K., 2020. Now is the time for a "great reset" of capitalism | World Economic Forum. World Economic Forum.

Sofaer, A., Clark, D., Diffie, W., 2010. Cyber security and international agreements. In: Proceedings of a Workshop on Deterring Cyberattacks. pp. 1–82.

State Security Agency, 2015. National Cybersecurity Policy Framework For South Africa 66–95.

Sutherland, E., 2017. Governance of Cybersecurity – The Case of South Africa. The African Journal of Information and Communication 83–112.

Thun, S., Kamsvåg, P.F., Kløve, B., Seim, E.A., Torvatn, H.Y., 2019. Industry 4.0: Whose revolution? The digitalization of manufacturing work processes. Nordic Journal of Working Life Studies 9, 39–57.

Van Niekerk, B., 2017. An Analysis of Cyber-Incidents in South Africa. The African Journal of Information and Communication 113–132.

Van Niekerk, B., 2019. The cyber security dilemma: A South African perspective. 14th International Conference on Cyber Warfare and Security, ICCWS 2019 441–447.

van Vuuren, J., Leenen, L., Plint, G., Zaaiman, J., Phahlamohlaka, J., 2017. Formulating the Building Blocks for National Cyberpower. International Journal of Cyber Warfare and Terrorism 7, 16–28.

Victoria, A., 2019. Cybersecurity on 5G Technology.

Wang, A.X., Hou, A., Warren, B., Popova, I., Shelepov, A., Sakharov, A., Ignatov, A., 2019. 2018 BRICS Johannesburg Summit Interim Compliance Report Prepared by 1–101.

World Economic Forum, 2020. Energy Policy Lighthouses: The Little Green Book.

Yunos, Z., Ahmad, R., Mohd Sabri, N.A., 2015. A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia. Information Security Journal 24, 15–23