sustainability

MDPI

*Article*

# Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa

**Masike Malatji [1], Annlizé L. Marnewick [1,*] and Suné von Solms [2]**

[1] Postgraduate School of Engineering Management, University of Johannesburg, Auckland Park, PO Box 524 Johannesburg, South Africa; masikem@gmail.com
[2] Department of Electrical & Electronic Engineering Science, University of Johannesburg, PO Box 524 Johannesburg, South Africa; svonsolms@uj.ac.za
* Correspondence: amarnewick@uj.ac.za

**Abstract:** The water and wastewater sector is an important lifeline upon which other economic sectors depend. Securing the sector's critical infrastructure is therefore important for any country's economy. Like many other nations, South Africa has an overarching national cybersecurity strategy aimed at addressing cyber terrorism, cybercriminal activities, cyber vandalism, and cyber sabotage. The aim of this study is to contextualise the water and wastewater sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment. This is achieved by conducting a detailed analysis of the international, national and sector cybersecurity stakeholders; legislation and policies; and challenges pertaining to the protection of the water and wastewater sector. The study found some concerning challenges and improvement gaps regarding the complex manner in which the national government is implementing the cybersecurity strategy. The study also found that, along with the National Cybersecurity Policy Framework (the national cybersecurity strategy of South Africa), the Electronic Communications and Transactions Act, Critical Infrastructure Protection Act, and other supporting legislation and policies make provision for the water and wastewater sector's computer security incidents response team to be established without the need to propose any new laws or amend existing ones. This is conducive for the immediate development of the sector-specific cybersecurity governance framework and resilience strategy to protect the water and wastewater assets.

**Keywords:** cybersecurity; cybercrime; legislation; policy; systems thinking; water



**Citation:** Malatji, M.; Marnewick, A.L.; von Solms, S. Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa. *Sustainability* **2021**, *13*, 291. https://doi.org/10.3390/su13010291

Received: 11 November 2020
Accepted: 23 December 2020
Published: 30 December 2020



## 1. Introduction

Goal 16 of the United Nations' (UN) 17 sustainable development goals is intended to "promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels" [1]. But peace, justice and strong institutions [1] require strengthening coordination among various international and domestic stakeholders. Critical infrastructure protection also requires the strengthening of coordination among international and domestic stakeholders. The United States of America (USA) defines critical infrastructure according to the 2013 Presidential Policy Directive No. 21, as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [2] (p. 37). The study has adopted this as the baseline definition of a critical infrastructure.

An example of a water-specific critical infrastructure is the Latvian water supply and sewerage enterprises association [3] which oversees 27 member organisations [4]. In Austria, there are approximately 5500 water utilities, 1900 community-based utilities, 165 water supply associations and 3400 water supply cooperatives [5]. Having a regularly updated inventory list of such critical infrastructures is a good practice [6]. However, an

effective cyberlegislation is not only vital for identifying and classifying but maintaining a country's infrastructure and protecting its citizens [6,7].

In many countries, the water and wastewater supply systems are classified as critical infrastructure as they are vital to national public health and economic security. Thus, prolonged interruptions of such critical infrastructures would naturally result in deteriorating public health and economic losses [5]. It is therefore crucial to understand the cybersecurity policy trends and discussions [7] to ensure proper coordination of cybersecurity activities in a country. This paper explores South Africa's water and wastewater sector cybersecurity responsibilities within the national and international policy context. This highlights how well-defined policy regulations in any country could ensure coordination of stakeholder roles and responsibilities for carrying out water-specific critical infrastructure cybersecurity activities. Thus, failure to define and implement effective cyberlegislation and policies could have devastating impact on the protection of water and wastewater critical infrastructure.

In South Africa, the government gazetted the National Cybersecurity Policy Framework (NCPF) in 2015, which aimed at addressing cyber terrorism, cybercriminal activities, cyber vandalism, and cyber sabotage [8,9]. As the overarching national cybersecurity strategy of South Africa [9], the NCPF provides a governance process and guidelines to respond to cybersecurity threats and attacks against the country [8,9]. In the cybersecurity domain, policies outline the objectives and limitations of a strategy [10] to provide for measures to be put in place for the protection, safeguarding, and resilience of assets [11]. Thus, adopting the most recent cybersecurity technologies is only effective when deployed within the guidelines of a clearly defined and enforceable policy [10]. Since the adoption of the NCPF, South Africa has been actively conducting cybersecurity assessments, audits, and readiness exercises in different public sector entities as part of the implementation of the cybersecurity strategy. Water and wastewater is one such sector that needs to conduct its own cybersecurity assessments, audits, and readiness exercises. Failure to conduct these periodically could increase the risk and intensify severity of a cyberattack to critical water infrastructure [12].

For example, an attacker may use the cyber kill chain—reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and action on their objectives—to gain entry into the victim's environment through the corporate information technology (IT) domain and then move laterally to the operational technology (OT) domain to launch attacks on critical infrastructure [13]. OT is a collective term for industrial control systems (ICSs), supervisory control and data acquisition (SCADA) systems, and other industrial monitoring and control processes [14,15]. ICSs and SCADA systems are essentially the backbone of critical infrastructures worldwide, including water supply systems, electricity grids, and transportation and telecommunication networks [16,17]. A well-documented cyberattack of a water supply system which took three months to detect occurred at the Maroochy water treatment plant in Australia [18]. This cyberattack took place in 2000, when SCADA systems began experiencing loss of communication, false alarms, and loss of pump controllability due to altered configurations [12,13,19]. This resulted in nearly 1 million litres of raw sewage spilling into rivers, parks, and residential areas, causing damage to the environment and costing society a lot of money [14,16,20,21].

The cyberattack example above demonstrates that cybersecurity can significantly affect sustainability. All three pillars of sustainability—social, environmental or ecological, and economic [19]—were impacted. The social pillar was impacted as a result of the raw sewage spillage in residential areas, including the grounds of a hotel [20]. The death of marine life and unbearable stench, as reported by the Australian Environmental Protection Agency [16], shows the extent to which the environmental pillar was affected. Lastly, all these damages cost the Maroochy Shire Council and the state of Queensland money to clean up and rehabilitate the environment. Thus, the economic pillar of sustainability was also greatly impacted upon. It is also clear from this incident that the sustainability pillars can also be viewed as three distinct and yet interacting systems [21]. That is, if one

system/pillar is compromised, the other two will be equivalently affected in an attempt to return to the natural state of equilibrium [22,23].

In light of this, the paper aims to contextualise the water and wastewater sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment of South Africa. This will determine if and whether there is a need to propose any new legislation and/or policies, or amend existing ones, to address the cybersecurity requirements of the sector. A systems thinking method is adopted to achieve the study's aim by examining the interrelationships between the water and wastewater sector and national cybersecurity legislative and policy environments as one system rather than independent and unrelated elements.

This introductory section provides the background and context of the study problem. The rest of the paper is structured as follows: Section 2 outlines the international, national (South Africa), and sector (South African water and wastewater sector) cybersecurity policy and legislative environments; Section 3 describes the systems thinking research methodology adopted in the paper to contextualise the water and wastewater sector's cybersecurity responsibilities within the South African cybersecurity legislative and policy environment; Section 4 presents the results; and Section 5 discusses the findings. The policy recommendations of the study are outlined in Section 6 and the conclusion presented in Section 7.

## 2. Cybersecurity Policy and Legislative Environment

A cybersecurity policy helps to chart a course of action for ensuring security of cyberspace by defining collective and individual regulatory, legal, technical, behavioural, organisational, and international responsibilities in pursuit of cybersecurity [24,25]. Cybersecurity is therefore a shared responsibility for national governments, economic sectors, and organisations and/or individual digital device end-users [26]. The shared cyber defence responsibilities are usually coordinated by nation states to develop capabilities to achieve cyber resilience, reduce cybercrime, and secure critical national infrastructure while developing industrial and technological resources for cybersecurity [27]. In this section, the researchers reviewed the international, national, and sector (water and wastewater) cybersecurity literature to identify the stakeholders involved and existing policy and legal environment.

### *2.1. International System*

In the digital era, cybersecurity is of paramount importance for economic competitiveness and continuity of trade for organisations of all types and sizes. As the United Nations Economic Commission for Europe (UNECE) [28,29] asserts, cyberthreats cut across any social and economic activities nationally, regionally, and internationally. It is therefore prudent to explore available international cybersecurity cooperation mechanisms for the protection of critical infrastructure, including water and wastewater critical infrastructure. Of particular focus in this section are the key international cybersecurity stakeholders involved, applicable laws, and the challenges encountered when implementing cybersecurity practices.

#### 2.1.1. International Cybersecurity Stakeholders

In the protection of critical water-related infrastructure cybersecurity webinar held on 18 November 2020 by the World Meteorological Organisation [30], it was indicated by one of the UNECE speakers that work encouraging common regulatory frameworks in specific sectors with critical impact on sustainable development is under way at the UN. This includes a report on the sectoral initiative on cybersecurity by the UNECE [28], albeit not one specifically focused on the water-related infrastructure sector. This makes the UN one of the important international cybersecurity cooperation stakeholders. In addition, some of the regional and other international stakeholders relevant to South Africa's cybersecurity endeavours were reviewed in Appendix A and are as follows:

- African Union

- African Network Information Centre
- Council of Europe
- Forum of Incident Response and Security Teams (FIRST)
- International Criminal Police Organisation (Interpol)
- International Telecommunication Union
- Southern African Development Community
- United Nations

The African Network Information Centre is missing in Appendix A and is regarded by Dlamini [31] as a relevant stakeholder on the African continent regarding security of cyberspace. The next section explores some of the available treaties and conventions governing international cybersecurity cooperation and the interrelationships between the stakeholders mentioned above.

#### 2.1.2. International Cybersecurity Laws

The 2001 Budapest Convention, which is the Convention on international cybercrime by member states of the Council of Europe and other non-member states [32], is the first international cooperation mechanism on issues relating to cybersecurity and cybercrime [33]. It attempts to provide signatory states with a common international policy to fight harmoniously against cybercriminals [34]. Of the 47 member states of the Council of Europe, only one—the Russian Federation—has not signed [35], citing infringement of its (internet) sovereignty [36]. Ireland and Sweden are the only two member states that have signed but never ratified [35].

There are several non-member states that have not signed and/or ratified the Budapest Convention. These include countries such as Brazil, Nigeria, and New Zealand. In the Brazil-Russia-India-China-South Africa (BRICS) bloc, only South Africa has signed the Convention but has never ratified [37,38]. Thus, the total number of signatures not followed by ratifications stands at three—South Africa, Ireland, and Sweden—as of 10 November 2020. In addition, the total number of ratifications now stands at 65 [35]. Since accession to the Convention is by invitation only for non-member states such as those in the BRICS bloc, no truly binding international cybersecurity and cybercrimes agreement is currently in place [33]. On the African continent however, the African Union (AU) adopted the AU Convention—Convention on Cyber Security and Personal Data Protection in June 2014 [36,38,39]. According to Coleman [39], the AU Convention provides a framework for personal data protection which member countries may transpose into their domestic legislation but requires at least 15 countries to be ratified and take effect. At the time of writing, the AU Convention had been signed by 14 member countries out of 55, and ratified by 8 [40]. South African has not yet signed the AU Convention.

There has since been other efforts for international cooperation regarding cybersecurity and cybercrimes, such as the UN General Assembly resolution 70/237 adopted on 23 December 2015 [41]; the world summit on the information society's (WSIS) Geneva Plan of Action [42]; Global Cybersecurity Agenda by the International Telecommunication Union [33]; the Open-Ended Working Group based on UN General Assembly resolution 73/27 [43]; and the Group of Governmental Experts (GGE) based on UN General Assembly resolution 73/266 [44]. South Africa is a member of the GGE and, along with 24 other member states, is expected to submit a final report to the UN General Assembly in 2021 [44]. In summary, some of the most pertinent international cybersecurity laws are as follows:

- The Budapest Convention
- The ITU Global Cybersecurity Agenda
- UN General Assembly resolution 70/237
- UN General Assembly resolution 73/27
- UN General Assembly resolution 73/266
- WSIS Geneva Plan of Action

Apart from the Budapest Convention of 2001, none of these international cooperation measures are binding as yet. This leaves the Budapest Convention on international cyber-

crime as the only treaty that is binding to its member states. Clough [33] (p. 725), however, cautions that the Convention is only effective when all member states have capacity in place to enact "domestic legislation across the spectrum of substantive and procedural laws and to put in place mechanisms for international cooperation." Some of the international cybersecurity implementation gaps and challenges in the water and wastewater sector are explored in the next section.

#### 2.1.3. International Water-Specific Cybersecurity Challenges

It was mentioned earlier that ICSs are essentially the backbone of critical infrastructures worldwide, including of the water and wastewater critical infrastructure. The introduction of cyber connectivity into ICS environments has increased the vulnerability of all types of critical infrastructures to cyberattacks [3,45–47]. Recently, the USA's cybersecurity and infrastructure security agency (CISA) [48] has reported compromises on critical infrastructures, government agencies, and private sector organisations through a third-party contractor network management tool called SolarWinds Orion platform. According to CISA [48], this advanced persistent threat (APT) [49] began approximately in March 2020, with evidence suggesting that there are additional initial access vectors other than the SolarWinds Orion platform. APTs are cyberattacks carried out repeatedly over an extended period of time by actors with significant resources and sophisticated levels of expertise [20].

The Australian and USA critical infrastructure cyberattacks point to supply chain compromises [11,25,50,51]. Some of the challenges of implementing cybersecurity safeguards on critical infrastructures, including the water and wastewater critical infrastructure, are summarised in Table 1.

**Table 1.** International water-related cybersecurity implementation challenges.

| Challenge | Description | Source |
| --- | --- | --- |
| Supply chain compromises | Third-party contractors and vendors are used as access vectors to the intended victim's computer networks. | [12,48,52] |
| Increased cyber connectivity | Introduction of internet communication protocols to industrial control systems (ICSs) exposes them to security risks through the IT domain. | [12,13,53] |
| False sense of security by obscurity | Older supervisory control and data acquisition (SCADA) systems were isolated from corporate IT networks. With increasing cyber connectivity, they become difficult to secure due to design for safety and performance. | [53,54] |
| Network misconfigurations | Vulnerable computer network as a result of the misconfiguration of the firewall and related tools. | [45,55,56] |
| No media protection enforcement | Data theft due to a lack of removable media policy enforcement. | [57] |
| Unsecured remote access | Remote access to ICSs through untrusted devices, usually by third-party contractors and vendors increases cyber risk. | [53,58] |
| Undocumented policies and procedures | Undocumented cybersecurity policies and procedures make enforcement and compliance difficult. This inevitably increases organisational cyber risk. | [20,56] |
| Untrained personnel | Training and awareness of staff achieves significant cybersecurity improvements. The opposite also applies. | [20,59,60] |

The above-mentioned challenges of implementing water-related and other critical infrastructure cybersecurity safeguards are mostly at an organisational level [61]. However, government policy and legislation and international cooperation on fighting cybercrime can help deter the would-be attackers in various ways. For example, they can regulate and help improve the information flows, enable collaborative interrelationships, highlight best practices for different sectors, track and monitor emerging cybersecurity technologies, and increase cyber risk awareness and training among citizens [26]. South Africa's national cybersecurity legislation and government policies are reviewed in this regard.

### *2.2. National System*

To develop an effective cybersecurity strategy for the water and wastewater sector, it is prudent to first understand policy discussions at the national level [7]. On 23 March 2012, the NCPF was adopted by the South African Cabinet [36,62–64] and gazetted by the Minister of State Security on 23 September 2015 [65]. As the national cybersecurity strategy, the NCPF has six key objectives that can be summarised as "centralise coordination of cybersecurity activities, by facilitating the establishment of relevant structures, policy frameworks and strategies in support of cybersecurity in order to combat cybercrime, address national security imperatives and to enhance the information society and knowledge-based economy" [65] (p. 15). The NCPF's supporting legislation and policies were reviewed to determine where and how the water and wastewater sector fits in, if at all.

A review of the NCPF has since been done by various other researchers over the years, as detailed in Appendix A of this paper. Appendix A could have excluded all work published prior to September 2015, which was when the NCPF was officially gazetted. This is because, as discussed in later sections, some of the conclusions drawn from such work might currently be invalid or partially valid due to subsequent insertions, substitutions, and/or repeals of some pieces of legislation supporting the NCPF, notwithstanding the mergers and renaming of some government departments. However, it was decided that the essence of the content of some of the previous research work—such as stakeholders involved, coordination structure, and perceived gaps and challenges—remained relevant. Appendix A therefore includes the NCPF review work from 2013 onwards, that is, the period after which the South African Cabinet adopted the NCPF in 2012.

#### 2.2.1. National Cybersecurity Stakeholders

Review work of the national cybersecurity stakeholders was conducted in Appendix A. Stakeholders that are mentioned multiple times in Appendix A are listed once below as either domestic or foreign. All other stakeholders are listed below without exception. It should thus be noted that not all of these are necessarily key stakeholders to the implementation of the national cybersecurity strategy. The domestic stakeholders relevant to the national cybersecurity endeavours as reviewed in Appendix A are as follows:

- State Security Agency (SSA)
  - Electronic Communications Security—Cyber Security Incidents Response Team (ECS-CSIRT)
  - Cybersecurity Centre
- Department of Communications and Digital Technologies (DCDT)
  - National Cybersecurity Hub
  - Cyber Inspectorate
  - National Cybersecurity Advisory Council
- Department of Defence (DoD)
  - Cyber Command
  - Centre Headquarters
- South African Police Service (SAPS)
  - Cyber Crime Centre
- Department of Justice and Constitutional Development
  - National Prosecuting Authority
- Department of Trade, Industry and Competition
- Department of Public Service and Administration
- Department of International Relations and Cooperation
- Department of Science and Innovation
- Public sector Cyber Security Incidents Response Teams (CSIRTs)
- Industry CSIRTs
- State Information Technology Agency

- South African Revenue Service

The key national and domestic stakeholders as defined in the NCPF can be represented, as shown in Figure 1. As shown in Figure 1 and delineated in the NCPF, the key organs of state that play a critical role in the implementation of the cybersecurity strategy [65] are dominated by the Justice, Crime Prevention and Security (JCPS) cluster [66]. According to the Government of South Africa [67], the JCPS cluster is made up of the Presidency, the Ministry of Defence and Military Veterans, the Ministry of State Security, the Ministry of Justice and Correctional Services, the Ministry of Police, the Ministry of Home Affairs, the Ministry of International Relations and Cooperation, the Ministry of Finance, the Ministry of Small Business Development, the Ministry in the Presidency for Women, Youth and Persons with Disabilities, and the Ministry of Social Development. In Figure 1, the bidirectional arrows are not reporting lines. They represent information flow within and outside the national cybersecurity system.

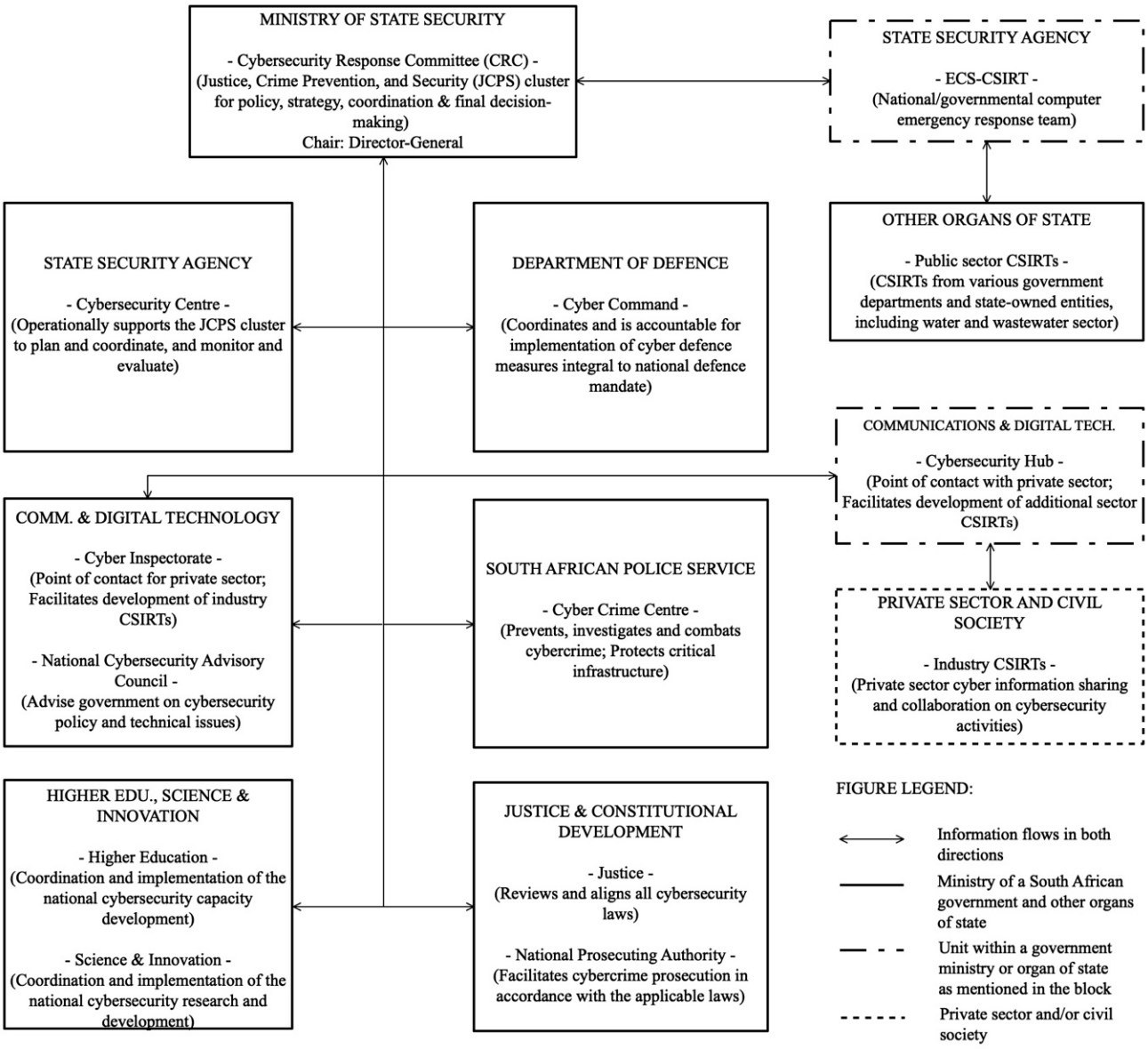


**Figure 1.** National cybersecurity governance structure in South Africa.

All other organs of state, including but not limited to those listed above, are required to align their cybersecurity and Information and Communications Technology (ICT) policies

and practices with the NCPF [65]. Effectively, Figure 1 shows the cybersecurity coordination and management structure in South Africa. The coordination is performed by the JCPS Cybersecurity Response Committee (CRC) [67] that is operationally supported by the Cybersecurity Centre in the SSA [65]. This inter-ministerial coordination is managed and facilitated through various pieces of legislation and government policies.

#### 2.2.2. National Cybersecurity Legislation and Policies

Review work of legislation and government policies used for the implementation of the national cybersecurity strategy was conducted in Appendix A. Similarly, pieces of legislation and policies that are mentioned multiple times in Appendix A are listed once below. All other pieces of legislation and policy are listed below without exception. It is therefore acknowledged that not all of these are necessarily key cybersecurity legislation and policies for the implementation of the national cybersecurity strategy. It is also acknowledged that not all cybersecurity-relevant legislation and policies are reflected in Appendix A. For example, as mentioned in the NCPF [65], the Electronic Communications Security Proprietary (Pty) Limited (Ltd) Act 68 of 2002 was not reflected in the review work in Appendix A. Nonetheless, the legislation and policies relevant to the national cybersecurity endeavours as reviewed in Appendix A are as follows:

- Constitution of the Republic of South Africa of 1996
- Broadband Infraco Act 33 of 2007
- Companies Act 71 of 2008
- Consumer Protection Act 68 of 2008
- Competition Act 89 of 1998
- Copyright Act 98 of 1978
- Corporate Governance of Information and Communications Technology Framework
- Critical Infrastructure Protection Act (CIPA) 8 of 2019
- Cryptography regulations
- Cybercrimes Bill of 2019 (waiting for assent by the President)
- Cyber Warfare Strategy
- Defence Review
- Designs Act 195 of 1993
- E-government strategy and roadmap (national)
- E-government strategy for each province
- Electronic Communications and Transactions Act 25 of 2002 (ECT Act)
- Electronic Communications Act 36 of 2005
- Films and Publications Act 65 of 1996
- Financial Intelligence Centre Act 38 of 2001
- Independent Communications Authority of South Africa Act 13 of 2000
- Inter-Governmental Relations Framework of 2005
- King IV Report on Corporate Governance
- National Archives and Record Service of South Africa Act 43 of 1996
- National Development Plan
- National Cybersecurity Policy Framework
- National Prosecutions Act 32 of 1998
- Prevention of Organized Crime Act 38 of 1999
- Promotion of Access to Information Act (PAIA) 25 of 2002
- Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004
- Protection of Personal Information (POPI) Act 4 of 2013
- Protection of State Information Bill
- Protection from Harassment Act 17 of 2011
- Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000
- Public Service Act: Regulation

- Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (or RICA)
- State Information Technology Agency Act 88 of 1998
- Trade Marks Act 194 of 1993

Achievement of the six key objectives of South Africa's national cybersecurity strategy is therefore distributed among 37, and probably more, different pieces of legislation and government policies [37,38]. This is the legal framework for national cybersecurity governance and resilience in South Africa. Harmonising and aligning these [37] could make the currently complex coordination and management of the national cybersecurity endeavours [38] a bit easier. In addition to the Constitution [68], it would appear from Appendix A that seven pieces of legislation and government policies in particular are key to the implementation of the national cybersecurity strategy as they are repeatedly mentioned. These are shown in Figure 2 [65,69–74].

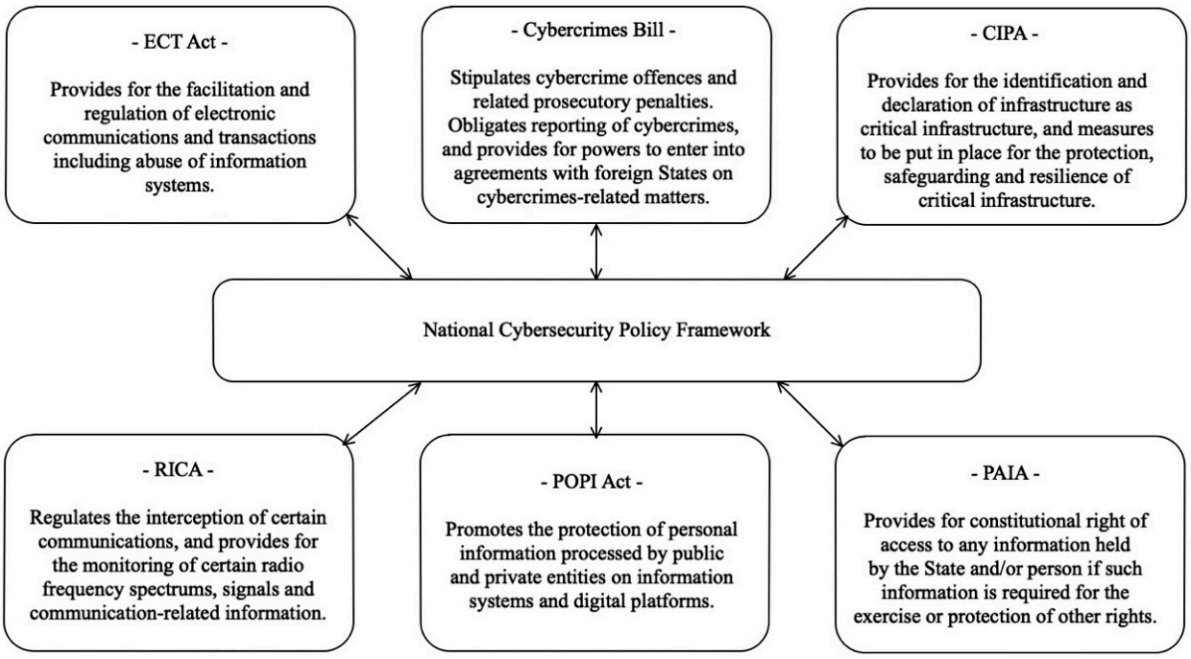


**Figure 2.** Key national cybersecurity policy and legislation in South Africa.

Review of the six individual pieces of legislation and one policy in Figure 2 revealed that some older laws—those enacted prior to the democratic dispensation in 1994—have since been repealed while others have been amended to respond to changing needs and to align with the country's constitution. It is worth highlighting a few of these in Table 2 as they relate to cybersecurity and cybercrimes in South Africa.

There are many other repeals and amendments but those are beyond the scope of the study. However, as one of the key cybersecurity laws in South Africa, it is imperative to highlight that, as shown in Table 2, sections 85 to 88 (cybercrime offences) of the ECT Act [73] have since been repealed and substituted by sections 2 to 12 of the newly approved Cybercrimes Bill [69]. Moreover, section 89 (cybercrime penalties) of the ECT Act has also been amended as outlined in section 58 of the Cybercrimes Bill. A review of the NCPF also revealed a few implementation gaps and challenges.

#### 2.2.3. National Cybersecurity Challenges

The review work in Appendix A revealed that, apart from the fact that the current coordination and management of the national cybersecurity strategy of South Africa is complex and should be simplified [37,38], a few challenges were identified. Although

Appendix A revealed more than ten gaps and challenges, these can be aggregated into the ten described in Table 3.

**Table 2.** National cybersecurity legislation amendments and repeals.

| Legislation | Current Status |
| --- | --- |
| Computer Evidence Act 57 of 1983 | Repealed by the ECT Act 25 of 2002. |
| Copyright Act 98 of 1978 | Amended after 1994. |
| Critical Infrastructure Bill of 2017 | Signed into law on 28 November 2019, and it is now the Critical Infrastructure Protection Act 8 of 2019 (Critical Infrastructure Act). |
| Cybercrimes and Cybersecurity Bill of 2017 | Revised and approved as the Cybercrimes Bill by the National Council of Provinces on 1 July 2020. |
| Monitoring and Prohibition Act 127 of 1992 | Repealed by RICA. |
| National Key Points Act 102 of 1980 | Repealed by CIPA. |
| Sections 85 to 88 of the ECT Act | Repealed and substituted by sections 2 to 12 of the newly approved Cybercrimes Bill. |
| Section 89 of the ECT Act | Amended as outlined in section 58 of the Cybercrimes Bill. |

Some of the challenges in Table 3 are similar to those experienced in other countries, for example, the limited collaboration and information sharing among various sectors and inadequate cybersecurity skills in Turkey [75]. Identifying and classifying critical infrastructure and updating the inventory on a regular basis is a challenge [6]. This is highlighted by White [2] in regards to the USA's Department of Homeland Security's need to develop guidelines to classify critical infrastructure sectors. In the case of Turkey, what [75] found was that if a sector is predominantly managed by private entities, the general cybersecurity posture tends to be more mature, and vice versa. In the case of the USA, however, the Department of Homeland Security is not a private entity. Perhaps cybersecurity issues are not that straightforward as stakeholder roles and responsibilities are often not as obvious, and moreover, the required security levels are also difficult to define [76]. The complex nature of the current coordination and management of the national cybersecurity strategy [37,38] may not be unique to South Africa after all. It is, however, important to understand how the cybersecurity gaps and challenges in Table 3 impact the water and wastewater sector's cybersecurity responsibilities. In this regard, the water and wastewater legal context was reviewed to determine whether and how it addresses protection of the sector's critical cyber infrastructure.

### *2.3. Sector System*

The Constitution of South Africa and specifically the Bill of Rights enshrines the basic human right to have access to adequate drinking water in section 27(1)(b), an environment that is not harmful to human health or well-being in section 24(a), and a healthy and safe environment in section 152(1)(d) [68]. These constitutional rights mandate the state in section 27(2) of the Constitution [68], through the Department of Water and Wastewater (DWS), to ensure that the water resources of the country are sustainably consumed and managed as well as protected [77].

**Table 3.** National cybersecurity challenges.

| Challenge | Description |
| --- | --- |
| Poor public-private partnerships track record | There is generally a poor track record of inter-ministerial coordination of government projects. It becomes even complex when stakeholders from industry, civil society, and special interest groups are involved. |
| Insufficient technical cybersecurity skills and user awareness education in South Africa | Development of technical cybersecurity skills must be prioritised by government. Public user education and awareness are pertinent aspects to preventing spoofing and phishing related cybercrimes in the country. |
| Independent and uncoordinated cybersecurity awareness initiatives | Currently, disparate and uncoordinated cybersecurity awareness training initiatives do exist. An integrated and coordinated approach to educating the public digital user about the dangers of cyberspace would be more effective. |
| Missing sector CSIRTs | With the exception of the banking sector which has the South African Banking Risk Information Centre (SABRIC), missing sector CSIRTs refers to the absence of CSIRTs in major sectors of the country, for example, in the mining, aviation, and agricultural sectors. These would be effective in sector information sharing and national coordination of cybersecurity incident responses. |
| Requirement for the establishment of new and dedicated cybersecurity institutions | The most critical cyber threats in South Africa are to the national critical infrastructure, intelligence agencies, and military. While the military and intelligence agencies are to some degree equipped to tackle cybersecurity, the provincial and local governments as well as the private sector operate and manage the vast majority of the national critical infrastructure. These entities must also be equipped to effectively protect the national critical infrastructure in a coordinated manner. This warrants the establishment of new and dedicated cybersecurity institutions. |
| Implementation of critical infrastructure protection still in abeyance | Protection of critical infrastructure is key in advanced cybersecurity strategies and must include strategies for cyber resilience and crisis management. Regulations are yet to be promulgated to implement the Critical Infrastructure Act. |
| Outstanding commitment to existing security conventions | There are no visible commitments to existing conventions such as the Budapest and African Union Convention on Cyber Security and Personal Data Protection. This would help in international collaboration on fighting cybercrimes, capacity building, and information sharing. |
| Lack of capacity and capability by law enforcement agencies | There is a huge gap between enacted laws and practical enforcement capability on the ground in most emerging and developing countries such as South Africa. This speaks to the point regarding the development of technical cybersecurity skills and user education and awareness. |
| Missing Cyber Inspectorate unit | A Cyber Inspectorate unit with powers to inspect, search, and seize cyber content in pursuit of unlawful digital acts was never established as clearly delineated in the ECT Act enacted in 2002. This is exacerbated by a poor track record of inter-ministerial coordination of complex government programmes. |
| International cooperation | South Africa is a non-member state signatory to the Council of Europe's international Convention on cybercrime—the Budapest Convention. However, a clear commitment to the Convention is lacking as it is yet to be ratified since its signing on 23 November 2001. |

#### 2.3.1. Water Stakeholders

Two water and sanitation strategic documents were reviewed to identify the stakeholders legally mandated to provide water and wastewater services in South Africa. These are the national water and sanitation master plan [78] and the latest Department of Water and Sanitation (DWS) annual report [77]. In these two documents, the key water and wastewater stakeholders from the public sector and their roles and responsibilities are clearly defined. The following are the identified key stakeholders in the water and wastewater sector of South Africa [77,78]:

- Parliament Portfolio Committee
- National Department of Water and Wastewater
- Regional Department of Water and Wastewater
- Provincial governments
- Local governments (municipalities as water service authorities, or water service providers through subcontractors)
- Water boards/regional water utilities
- Catchment management agencies
- Water-user associations
- Water Research Commission
- Trans-Caledon Tunnel Authority
- Water Tribunal
- Water trading entity

Note that the water boards/regional water utilities, catchment management agencies, water service authorities, water service providers and water-user associations are stakeholder categories that represent many water organisational entities. For example, the water service providers category includes both the public and private sector entities. Thus, the stakeholder categories above are representative of all the key stakeholders in the water and wastewater sector of South Africa. In addition to the stakeholders, the appropriate water legal framework is required for ensuring that the water resources of the country are sustainably consumed, managed, and protected.

#### 2.3.2. Water Legislation and Policies

Sources from [79–82] were reviewed to identify legislation and policies governing the water and wastewater sector of South Africa. Similar pieces of legislation and government policies in the sources were listed once below. All other pieces of legislation and policies are listed without exception below:

- Constitution of the Republic of South Africa of 1996—Chapter 2, sections 10, 24(a), 27(1)(b), 27(2), and 152(1)(d); Chapter 6, section 139(1); Chapter 7, section 154(1); Schedule 4, Part B
- Housing Act 107 of 1997
- National Water Act 36 of 1998
- Water Services Act 108 of 1997
- Water Research Act 34 of 1971
- National Environmental Management Act 107 of 1998
- Local Government: Municipal Structures Act 117 of 1998
- Local Government: Municipal Systems Act 32 of 2000
- Strategic Framework on Water Services of 2003
- Chapter 4 of the National Development Plan
- National Water Policy Review of 2013
- National Wastewater Policy of 2016
- Water and Wastewater Climate Change Policy of 2017
- National Water Resources Strategy, Second Edition, of 2013
- White Paper on Basic Household Wastewater of 2001
- White Paper on National Water Policy for South Africa of 1997

- White Paper on Water Supply and Wastewater of 1994
- National Water and Wastewater Master Plan of 2019

The words "secure", "security" and "protection" were searched in each of the pieces of legislation and policies above. The idea was to determine if and whether provisions for cyber critical infrastructure protection are made. The review revealed water cybersecurity gaps and challenges as discussed in the next section.

#### 2.3.3. Water Cyber Critical Infrastructure Protection Challenges

A review of the legislation and policies identified in the previous section revealed that their purposes are essentially about providing for an integrated water resources management agenda [83]; a technique for planning, monitoring, and managing water resources in a coordinated manner. The legislation and policies contain nothing relating to the protection of critical cyber and physical infrastructure as described in Table 4.

**Table 4.** Water cyber critical infrastructure protection challenges.

| Challenge | Description |
| --- | --- |
| National Water Act provides for protection of raw water | This does not refer to the protection of raw water cyber critical infrastructure. Instead, it refers to the planning, monitoring and managing of water resources in a coordinated manner. |
| The Strategic Framework on Water Services of 2003 provides for protection of water assets | This does not refer to the cyber protection of water assets. Instead, it refers to the repair, maintenance, and rehabilitation of water systems. |

Table 4 indicates that the closest reference to some kind of protection is in the National Water Act, which in addition to the protection of raw water in South Africa, provides for the governance of raw water, including the development, consumption, management, and control of aquatic ecosystems [78]. The Strategic Framework on Water Services of 2003 also mentions protection of water assets albeit as it pertains to the repair, maintenance, and rehabilitation of water systems. Therefore, no provision for critical cyber and physical infrastructure protection is made in all the water and wastewater legislation and policies. A review of the existing international, national, and sector (water and wastewater) cybersecurity legislative and policy environments has been conducted in this section. The review identified the national and water and wastewater sector cybersecurity gaps and challenges. What is not clear thus far is how the water and wastewater sector interrelates with the national cybersecurity legislative and policy environment.

### *2.4. Systems Interrelationships*

The previous sections discussed three interdependent cybersecurity systems, each with its own unique purpose. These were the international, national, and sector cybersecurity systems. The interdependent relationships between these dynamic systems as well as how they can interoperate effectively is illustrated in Figure 3 as derived from [26].

The arrows in Figure 3 represent cybersecurity information flow within and between the three interdependent systems. Clough [33] indicated that nation states should put in place domestic legislation that is conducive for international cooperation such as the Budapest Convention. Coleman [39] concurs with this and argues that collaborations such as the AU Convention on Cyber Security and Personal Data Protection provide a legal template that could be aligned with but also customised according to domestic legislation and policy requirements. This indicates that the dynamic relationships within and between the three systems are governed by legislation and government policy. While the international and national systems in Figure 3 have clear cybersecurity-related policies and/or legislation, no cybersecurity-related legislation and/or government policy is defined specifically for the water and wastewater sector. By utilising the systems thinking approach, the interrelationships between the water and wastewater sector (sector system

in Figure 3) and national cybersecurity legislative and policy environment (national system in Figure 3) were examined further. The research methodology on how to achieve this is described in the next section.

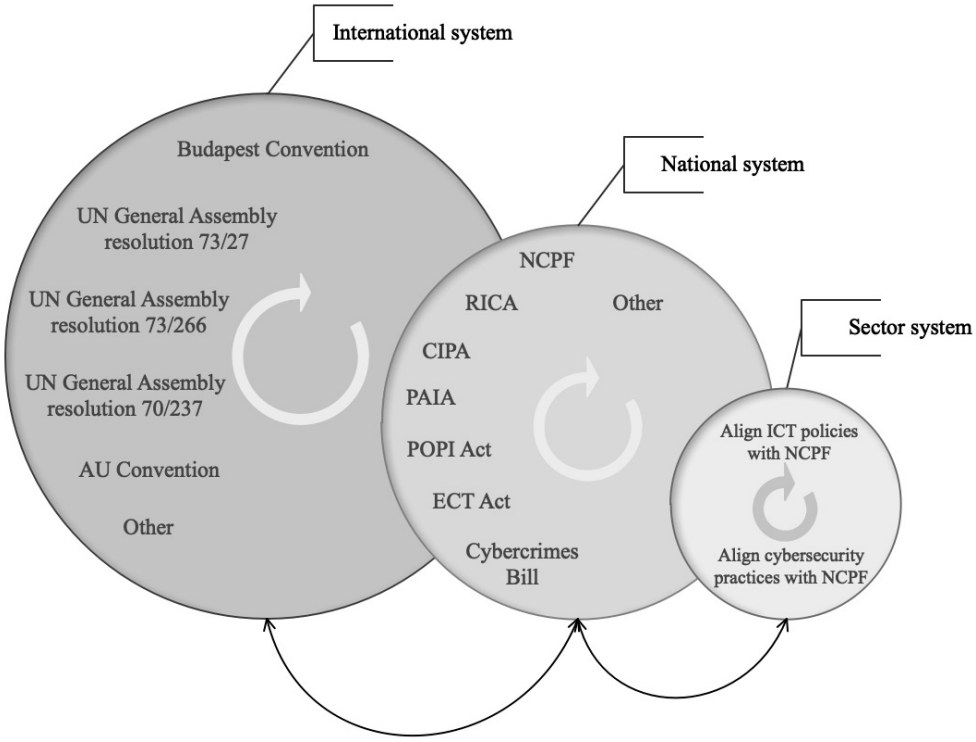


**Figure 3.** Cybersecurity systems dynamic interrelationships.

## 3. Materials and Methods

The systems thinking approach [84,85] is employed to achieve the research aim of this study. The approach is deemed suitable as it helps examine dynamic patterns and events by holistically focusing on the interrelationships between a system's parts rather than seeing the constituent parts as static, standalone, and unrelated elements [84,85]. It is an analysis tool to identify and understand how the parts interconnect within the entire system [86]. This is especially useful when considering the complex nature of government policy and the different parties involved in effecting legislation. In this study, a system is perceived as a group of interdependent elements assembled to create an emergent character or behaviour of the group as a whole [22,23,87,88]. As shown in Figure 4, the national cybersecurity strategy of South Africa is considered a system in this study, and its underlying structure comprises three main parts: (i) Function; (ii) Elements; and (iii) Interconnections.

Firstly, the stated function of a system is its purpose, which sets out how that system is expected to behave [87]. Altering the function of a system has the greatest impact on the entire system and may render it unrecognisable [84]. Secondly, the elements of a system are the most visible and are the actors in the system [87]. It is however acknowledged that some elements can be more important than others [84]. Changing system elements has the least impact on a system [84], provided that the function of the system remain unaltered [87]. Thirdly, interconnections are oftentimes harder to see but more critical in the system than elements [84,87]. They are the signals that enable one element of a system to respond to other elements through action or decision points [84]. Oftentimes, interconnections are not physical flows [84,87], but rather the flow of influences, energy, or information inside and outside the system as it strives towards a state of equilibrium [22,23]. The interconnections of a system's elements are configured in such a way as to generate their own characteristic or emergent behaviour, which may start to differ from the espoused or defined purpose [22,84,87]—which is why systems are firm and very difficult to change [89].

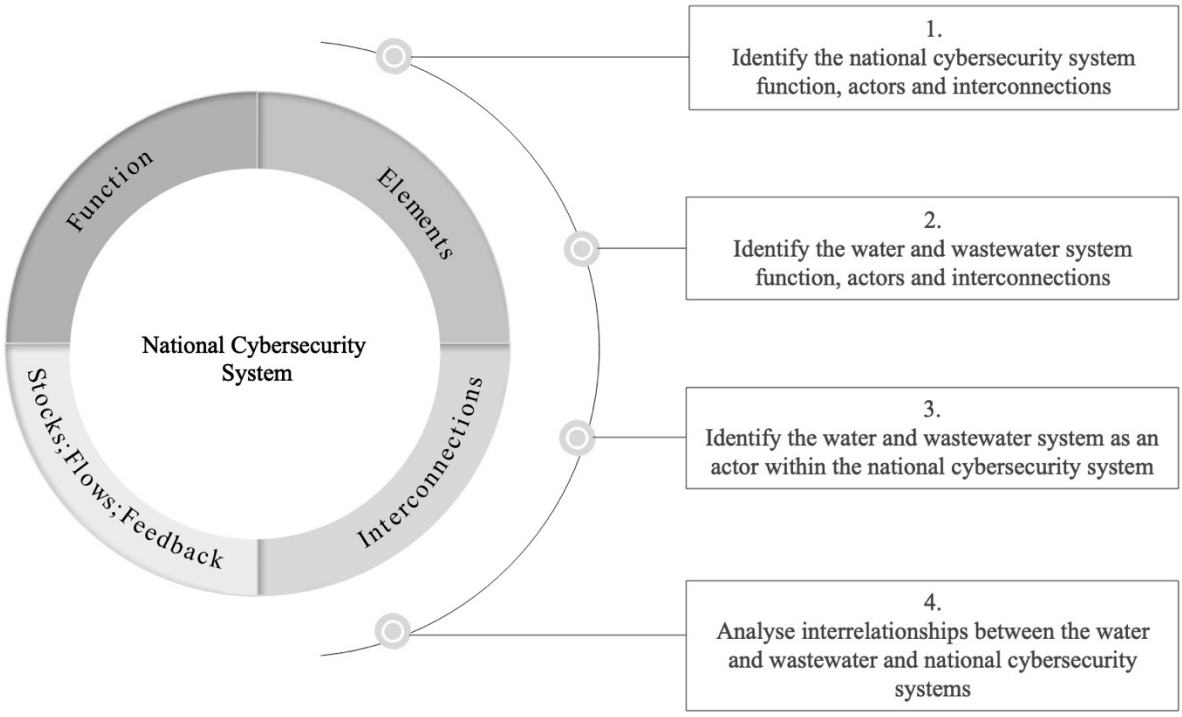


**Figure 4.** Systems thinking approach.

In addition to system elements/actors, interconnections and function, three more parts make up a system [84]: (i) Stocks, which are the snapshots or historical views of a system, showing the changing flows in the system; (ii) Flows, which are the inflow and outflow activities of a system impacting the levels of stock; and (iii) Feedback loops, which occur when a change—reinforcing or balancing loop [85]—in stock levels leads to additional positive or negative changes [84,87,89,90]. However, these did not form the central aim of the study. To closely examine the interrelationships between the water and wastewater sector and national cybersecurity legislative and policy environment, the four steps in Figure 4 are sequentially operationalised.

Ultimately, the goal of a systems thinking approach is leverage—identifying where changes and concomitant actions in the underlying structure of a system can result in significant and lasting improvements [86]. In the next section, a review of the national and sector cybersecurity literature is conducted to identify the underlying structure of the national cybersecurity system. This should shed light on the key stakeholders and government policies and legislation required to realise significant and lasting improvements to national and, more specifically, water and wastewater sector, cybersecurity endeavours.

## 4. Results

In this study, South Africa's water and wastewater sector and the national cybersecurity legislative and policy environment were analysed. The analysis was conducted to contextualise the water and wastewater sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment and determine whether there is a need to propose any new legislation and/or policies, or amend existing ones, to address cybersecurity requirements of the sector. The findings are summarised in Table 5.

In Table 5, the "international cybersecurity system" means the international laws and stakeholders on fighting cybercrime, and the "national cybersecurity system" means the South African cybersecurity legislative and policy environment inclusive of key stakeholders. Similarly, the "water and wastewater sector as a system" means the water and wastewater legislative and policy environment inclusive of the sector's key stakeholders, and the "water and wastewater sector as a stakeholder" means the sector as one of the

key stakeholders within the national cybersecurity system. The findings in Table 5 are discussed in the next four sections.

**Table 5.** Summary of study findings.

| | Cybersecurity Purpose (System Function) | Cybersecurity Stakeholders (System Elements/Actors) | Cybersecurity Legislation and Policies (System Interconnections) |
|---|---|---|---|
| International cybersecurity system | Defined | Partially defined | Partially defined |
| National cybersecurity system | Defined | Defined | Defined |
| Water and wastewater sector as a system | Not defined | Not defined | Not defined |
| Water and wastewater sector as a stakeholder | Defined | Defined | Defined |

### *4.1. Identify the National Cybersecurity System Function, Actors and Interconnections*

The purpose of this analysis exercise was to identify key national cybersecurity stakeholders (actors) responsible for the implementation of the six key objectives of the national cybersecurity (function), as well as to identify legislation and policies (interconnections) governing the interrelationships among stakeholders. The function of the national cybersecurity strategy has already been defined in Section 2.2 as to "centralise coordination of cybersecurity activities, by facilitating the establishment of relevant structures, policy frameworks and strategies in support of cybersecurity in order to combat cybercrime, address national security imperatives and to enhance the information society and knowledge-based economy" [65] (p. 15). On the one hand, the national cybersecurity strategy function is implemented by domestic stakeholders such as the SSA, SAPS, and DCDT supported by foreign stakeholders such as the African Union, Interpol, and FIRST. The national cybersecurity stakeholders are the defined actors or elements of the national cybersecurity system.

On the other hand, six key pieces of legislation—such as the ECT Act, Cybercrimes Bill, and POPI Act—and one policy, the NCPF, were found to determine the interrelationships among the stakeholders in the national cybersecurity system. These are the interconnections of the national cybersecurity legislative and policy environment. As argued by Sutherland [38] and Detecon [37], the current coordination and management of the national cybersecurity programme is complex. To demonstrate how complex the current implementation of the national cybersecurity strategy is, a few gaps and challenges were identified in the national cybersecurity legislation and policy environment. These are summarised as follows:

- Subsections 16.4(b) and 16.4(c) of the NCPF mandate the DCDT to establish the National Cybersecurity Advisory Council and Cybersecurity Hub, which in turn is tasked to encourage and facilitate the establishment of industry CSIRTs, whereas Chapter 12 of the ECT Act mandates the same government department to establish a Cyber Inspectorate unit and appoint cyber inspectors. Firstly, no Cyber Inspectorate unit has ever been established and no cyber inspectors were ever appointed to date. Secondly, except for the banking industry, which has SABRIC, there are few other industry CSIRTs, even those are not actively coordinated for information sharing and incidents recording in a national database. Lastly, the National Cybersecurity Advisory Council is non-existent or at least its activities, if any, are not visible.
- The NCPF recognises and encourages cybersecurity education for technical skills development, user awareness campaigns, and research and development in Section 2.7 of the policy. However, there are no visible and coordinated nation-wide activities to address insufficient technical cybersecurity skills and user awareness campaigns in the country.

- The CIPA provides for infrastructure resilience, albeit without explicitly stating whether this includes cyber resiliency. Moreover, the SAPS is yet to develop regulations to implement the Act.
- Despite the existence of the different pieces of cybersecurity-related legislation and policies, there seems to be a lack of capacity and capability by law enforcement agencies in fighting cybercrimes in South Africa.

### *4.2. Identify the Water and Wastewater System Function, Actors and Interconnections*

The purpose of this analysis exercise was to identify all the important stakeholders (actors) for the provision of quality water and wastewater services as well as cyber protection of the water infrastructure (function), which legislation and policies (interconnections) are responsible for the functions, and whether these delineate cybersecurity-related roles and responsibilities. On the one hand, the key stakeholders, such as the DWS, water boards and Trans-Caledon Tunnel Authority responsible for the provision of quality water and wastewater services, were identified in Section 2.3.1. On the other hand, pieces of legislation, such as the National Water Act, Water Services Act and Water Research Act, and policy, such as the National Water and Wastewater Master Plan, were identified in Section 2.3.2. These determine the interrelationships among the stakeholders in the water and wastewater sector for the provision of quality water and wastewater services. However, further analysis revealed that no cybersecurity-related roles and responsibilities are defined in the water and wastewater sector legislation and policies. This means that the water and wastewater sector is what SEBoK Editorial Board [88] refers to as an independent system (see sector system in Figure 3) comprised of its own components configured in such a way as to achieve its unique purpose within the national system.

### *4.3. Identify the Water and Wastewater System as an Actor in the National Cybersecurity System*

The purpose of this analysis exercise was to identify which of the national cybersecurity stakeholders represent the water and wastewater sector. Analysis revealed that the *Public sector CSIRTs* in the 'OTHER ORGANS OF STATE' block in Figure 5 represents the water and wastewater sector as an actor or stakeholder within the bigger national cybersecurity system. Moreover, all national, provincial, and local government departments as well as state-owned entities are also represented by the public sector CSIRTs. As shown in Figure 5, the public sector CSIRTs have a direct interconnected relationship with the ECS-CSIRT located in the SSA.

According to Sutherland [38], the ECS-CSIRT is actually Electronic Communications Security (Pty) Ltd. or COMSEC Pty Ltd., a private enterprise established in 2002 and mandated by the SSA to ensure protection of critical electronic communications. Like many other public sector and industry CSIRTs, the water and wastewater sector CSIRT is yet to be established. Since no cybersecurity-related roles and responsibilities are defined in the water and wastewater legislative and policy environment, only one option is left: the national cybersecurity legislative and policy environment. To determine whether and how the existing national cybersecurity legislative and policy environment delineates the water and wastewater cybersecurity responsibilities, the interconnected relationships between the two systems were analysed.

### *4.4. Analyse Interrelations between the Water and Wastewater and National Cybersecurity Systems*

The purpose of this analysis exercise was to determine if and whether the existing national cybersecurity legislation and government policies delineate water and wastewater cybersecurity role and responsibilities. It was found that the water and wastewater legislation and policies give no provision for the sector's critical cyber and physical infrastructure protection. Instead, analysis revealed that the cybersecurity roles and responsibilities to provide for the sector's critical cyber and physical infrastructure protection, and indeed those of other sectors, are drawn mainly from the NCPF [65], Cybercrimes Bill [69], CIPA [70], POPI Act [71], RICA [72], ECT Act [73], and PAIA [74]. For example, the NCPF states that

the SSA shall, among other things, be required to "initiate and lead a process" [65] (p. 27) for the establishment of public sector CSIRTs while the Cybersecurity Hub at the DCDT should do the same with private sector CSIRTs and civil society stakeholders [65] (p. 18).

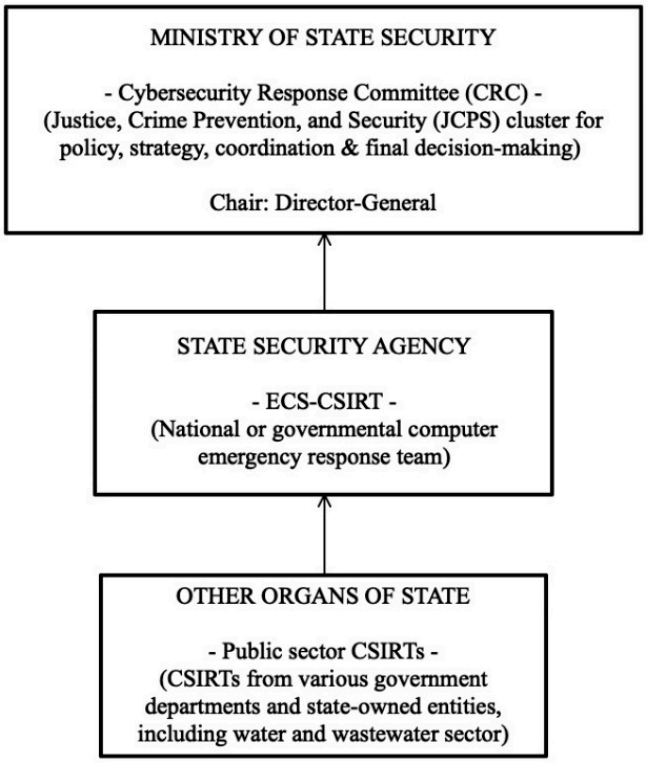


**Figure 5.** Water and wastewater system as an actor within the national cybersecurity system.

It has already been established in the previous section that the water and wastewater sector is represented by the public sector CSIRTs block in the national cybersecurity governance structure. The cybersecurity roles and responsibilities of sector CSIRTs are delineated in Section 6.3.6 of the NCPF and require, among others, that sector CSIRTs "establish national security standards and best practices for the sector in consultation with the Cybersecurity Centre (located in the Ministry of State Security) and the JCPS CRC, which are consistent with guidelines, standards and best practices developed in line with the NCPF" [65] (pp. 18–19). Along with other defined roles, this role interconnects the water and wastewater sector as an actor with other stakeholders or actors/elements inside and outside the national cybersecurity system to achieve the nation's function or purpose of securing against cyberattacks. Additionally, cybercrimes and concomitant penalties from such cyberattacks are defined in the Cybercrimes Bill and ECT Act as supported by other mentioned key legislation and policies. These are the interconnections of the national cybersecurity and water and wastewater systems. Therefore, the water and wastewater system's cybersecurity purpose, stakeholders, and legislation and policies are only defined when the sector is an actor—public sector CSIRT—within the national cybersecurity system. The ramifications of these findings as they pertain to the aim of the study are therefore discussed in detail.

## 5. Discussion

The aim of this study was to contextualise the water and wastewater sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment. To achieve the aim, systems thinking was adopted to analyse the purpose or function of both the national cybersecurity and water and wastewater systems, stakeholders involved to achieve the functions, and stakeholder interrelation. The ramifications of the study

findings are discussed under two headings: (i) National cybersecurity legislative and policy environment; and (ii) Water and wastewater legislative and policy environment.

*National cybersecurity legislative and policy environment*. The study findings indicate that the function of the national cybersecurity system is clearly defined in the NCPF. The purpose of the national cybersecurity strategy is therefore very clear. According to Meadows [84], altering the function of a system has the greatest impact on the entire system and may render it unrecognisable. This means that changing the purpose of the national cybersecurity strategy has the greatest impact on the entire national cybersecurity programme. The findings also indicated that the JCPS CRC was established to oversee the implementation of the national cybersecurity strategy by ensuring consistency with guidelines, standards and best practices developed in the NCPF. The JCPS CRC is the key stakeholder or element/actor in the national cybersecurity system. Although it is acknowledged that some key stakeholders can indeed be more important than others [84], systems thinking indicates that changing individual stakeholders should have the least impact on the national cybersecurity programme provided that the purpose and legislation and policies remain unaltered. This means that stakeholders implementing the national cybersecurity strategy, including individual members of the JCPS CRC, can be changed without having a noticeable impact on the overall purpose of the programme.

Furthermore, the findings indicated that the flow of information among and between the national cybersecurity stakeholders is governed by legislation and policies such as the Cybercrimes Bill, CIPA, ECT Act, NCPF, POPI Act, RICA, and PAIA. In terms of international cybersecurity cooperation, South Africa is yet to ratify the Budapest Convention of 2001 as of 10 November 2020 [35]. That leaves Interpol and extradition treaties between South Africa and other countries as the only available international cooperation mechanisms to fight cybercrimes perpetrated outside its jurisdiction. Systems thinking indicates that each legislation and/or policy interconnects stakeholders in such a way that it could generate its own characteristic or emergent behaviour, which may start to differ from the espoused or defined purpose of the national cybersecurity strategy. This means that amending or repealing cybersecurity-related legislation and government policy could have significant impact on the overall purpose and performance of the national cybersecurity programme. This is why it was important to dig deeper to understand the interconnected relationships among the stakeholders involved and the impact these relationships have on the overall purpose and performance of the national cybersecurity programme. What the findings show is that a seamless coordinated effort is required to implement the national cybersecurity strategy. The argument that government has a below par performance record when it comes to the implementation of policies involving several government stakeholders and requiring public-private partnerships [91] is not encouraging. It was also found that the no less that 37 different pieces of legislation and policies led to further implementation gaps and challenges. The ramifications of these gaps and challenges, which also impact on the water and wastewater sector's cybersecurity responsibilities, are fourfold.

Firstly, since the enactment of the ECT Act in 2002, the DCDT has failed to establish the Cyber Inspectorate unit and appoint cyber inspectors, failed to report any activities by the National Cybersecurity Advisory Council, if any, and progresses slowly to ensure the establishment of industry and sector CSIRTs as stipulated in the NCPF since it was gazetted in 2015. All these shortcomings point to a lack either of capacity or capability by the DCDT, or a combination of both.

Secondly, tasked to be the national structure dedicated to cybersecurity activities, including cybersecurity technical skills and user awareness campaigns and engagement with the private sector and civil society, the DCDT's Cybersecurity Hub is visibly absent in the coordination of these activities. As already alluded to by Detecon [37] and corroborated by Gcaza [92], cybersecurity awareness and education have proven to be effective in significantly reducing the risk of a security breach. This is because awareness and education prepare technical experts to put proactive safeguards in place, and ordinary end-users to be consciously alert. The case in point on the importance of cybersecurity awareness

and education is the data breach at Experian South Africa, a credit records organisation, where a database containing personal details of approximately 24 million consumers and nearly 800,000 businesses was willingly handed over to a fraudster [93] as a result of a social engineering attack. Thus, the national government, and in particular the water and wastewater sector, should develop a strategy to embark on a coordinated effort to achieving the required sector cybersecurity skillset. This investment is fully supported and encouraged in Section 2.7 of the NCPF. This lack of visible and strategic coordination by the Cybersecurity Hub also points to a lack either of capacity or capability within the DCDT.

Thirdly, the regulations to promulgate the CIPA had not yet been gazetted by the SAPS at the time of writing. In terms of the transitional arrangements in the Act, Parliament must first approve the SAPS draft regulations. Until that happens, the Act is held in abeyance [94]. In this regard, it is not yet clear which national assets per sector, including the water and wastewater sector, will be identified and classified as national critical infrastructure. Perhaps when the CIPA regulations are gazetted, the roles, responsibilities, and accountability of different parties will be defined to also include cyber resilience. As argued by Mutemwa [66], a good cybersecurity strategy should also include cyber resilience in addition to cyber defence policies and capabilities. A cyber resilience strategy helps shift from a retroactive to a more proactive approach [95]. As matters currently stand, the CIPA merely promises to enable the protection and safeguarding of critical infrastructure to achieve resiliency. How that critical infrastructure resilience is going to be achieved with cooperation between government and the private sector remains unclear.

Lastly, the findings suggest a clear lack of capacity and capability by law enforcement agencies in fighting cybercrimes in the country. This might require a coordinated cybercrimes skills development collaboration programme with international stakeholders such as Interpol and similar others to help bridge the gaps in the short term. In addition to all the matters considered above relating to the national cybersecurity legislation and policy environment, there is another concern: It would appear that the national cybersecurity strategy is primarily more defensive [8], and thus retroactive, than offensive which requires proactiveness [96]. It is more passive and static than proactive. Under international laws, any sovereign state has the right to defend itself against adversarial actors [96]. As the national cybersecurity policy overarching both the DoD's Defence Review and Cyber Warfare Strategy, the NCPF does not explicitly state whether South Africa would execute cyber offence strategies in response to a cyberattack. Even in its delineation of the role and responsibilities of the DoD, the NCPF refers to the development of a "Cyber Defence Strategy, that is informed by the National Security Strategy of South Africa" [65] (p. 24). Defence (retroactive approach) seems to be our cybersecurity strategy as opposed to adopting an offensive (proactive approach) or a combination of both strategies.

In spite of these national cybersecurity challenges, the Cybercrimes Bill, CIPA, ECT Act, NCPF, POPI Act, RICA, and PAIA, together with other cybersecurity-relevant legislation and policies, are drafted in such a way as to address the cybersecurity requirements of the water and wastewater sector without the need to propose any new legislation and/or policies or amend existing ones. All the sector needs to do is to encourage member organisations to align their ICT policies and cybersecurity practices with the NCPF to address cyber risks and water-related cybersecurity implementation challenges such as those highlighted in Table 1.

*Water and wastewater legislative and policy environment*. The study findings indicate that the water and wastewater sector has two functions fulfilled through two different stakeholder responsibilities. The first function is that the water and wastewater sector is mandated to supply quality water and wastewater services to the nation. This function or purpose is achieved through the water and wastewater sector as an independent system comprised of its own stakeholders (system elements/actors)—such as DWS, water boards, and Trans-Caledon Tunnel Authority)—and legislation and policies (interconnections)—such as the National Water Act, Water Services Act, and National Water and Wastewater Master Plan. The second function is that the water and wastewater sector has national

cybersecurity responsibilities. This function is achieved by the water and wastewater sector as a stakeholder—public sector CSIRT—in the bigger national cybersecurity system. The public sector CSIRT cybersecurity responsibilities of the water and wastewater sector are defined in Section 6.3.6 of the NCPF [65].

The findings also indicated that the public sector CSIRT will report to the national CSIRT or ECS-CSIRT in the SSA. It is not clear whether the ECS-CSIRT caters for both corporate IT and ICS cybersecurity services nor how, specifically, it helps the public sector CSIRTs as it claims on its website. The roles and responsibilities defined in the NCPF [65] (pp. 18–19) further require that the Cybersecurity Centre located in the SSA be consulted by public sector CSIRTs when establishing national security standards and best practices for their sectors. The question is, what is the relationship between the Cybersecurity Centre and ECS-CSIRT, both located in the SSA? Is COMSEC (Pty) Ltd. now the Cybersecurity Centre? Are they different? To reiterate Sutherland's [38] point, perhaps this is what contributes to the complex manner in which the national cybersecurity strategy of South Africa is being implemented. Nonetheless, it has already been proven that the existing national cybersecurity legislative and policy environment provides for the establishment of the water and wastewater sector-specific CSIRT without the need to propose any new laws or amend existing ones. However, this is based on the assumption that the DWS will host the CSIRT on behalf of the entire sector. Whether this is the best way to do it is a separate discussion. Alignment of the sector's ICT policies and cybersecurity practices with the NCPF is enough to establish a CSIRT that will be hosted at the DWS.

By understanding the dynamic nature of its interconnected relationships [23,85,97] among various stakeholders, the water and wastewater sector is therefore immediately able to develop its own cybersecurity governance framework and resilience strategy as illustrated in Figure 6.

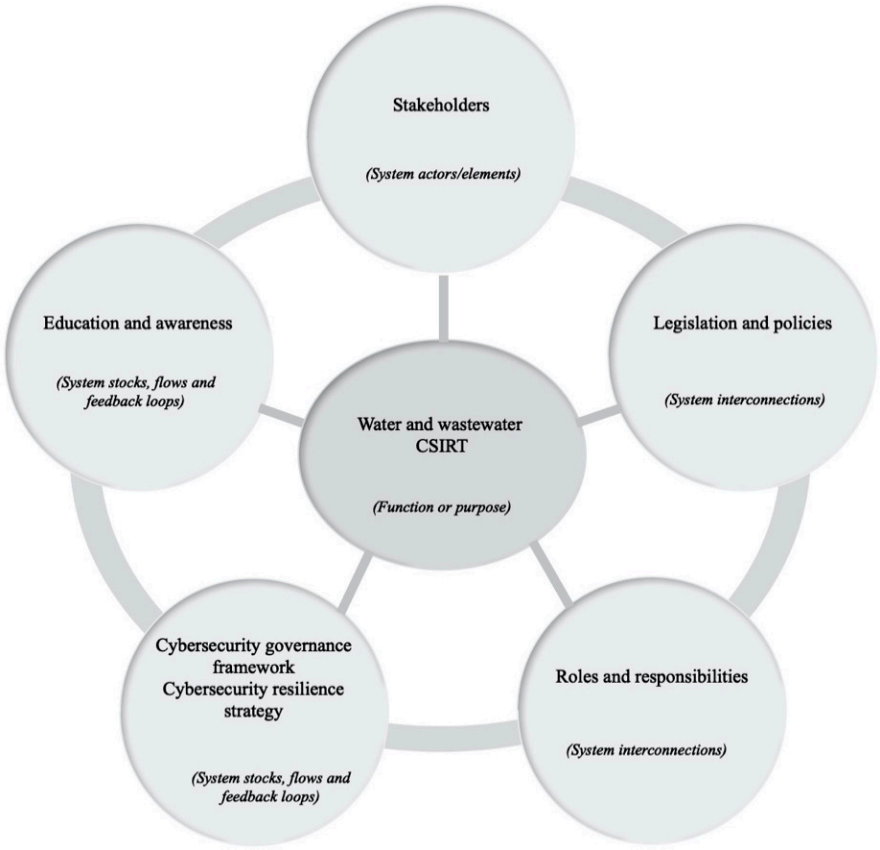


**Figure 6.** Water and wastewater cybersecurity system.

De Jong et al. [98] assert that outsiders usually offer creative and innovative policy inputs that can lead to a better understanding of societal challenges. This approach yields better policy decisions with more realistic judgements of the advantages and disadvantages of potential policy measures [98,99]. The water and wastewater sector should therefore be as collaborative with "outsiders" such as the JCPS CRC, Cybersecurity Hub in the DCDT, and Cybersecurity Centre in the SSA and as representative (among its member organisations) as possible in order to attain, through better policy decisions, the desired level of sector cybersecurity resiliency against cyber threats and attacks. In this regard, policy recommendations are proposed as outlined in the next section.

## 6. Recommendations

The study has a few recommendations regarding the national cybersecurity legislation and policy environment and the water and wastewater sector's cybersecurity responsibilities within this legal context. Firstly, regarding the national cybersecurity legislation and policy environment, the following are recommended:

- The National Cybersecurity Advisory Council, and/or Cybersecurity Hub, and/or Cyber Inspectorate unit should either be moved from the DCDT, or their operating models and mandates be reviewed, or a combination of both.
- The Critical Infrastructure Protection Act should be amended to explicitly include "cyber" and/or "digital or information" infrastructure in its definitions of "infrastructure" and "critical infrastructure" terms.
- To boost capacity and capability in fighting cybercrimes in the sort-term, South African law enforcement agencies may need to partner with international stakeholders such as Interpol and similar others to develop cybercrimes and digital forensics skills. For medium to long term solutions, the law enforcement agencies should recruit the best and brightest students with passion and a keen interest in cybercrimes and digital forensics from local universities.

Lastly, regarding the water and wastewater sector's cybersecurity responsibilities within the national cybersecurity legislation and policy environment, the following are recommended:

- *Establish a sector computer security incidents response team*. Establish the national water CSIRT that will have specialist teams serving both the IT and ICS cybersecurity requirements to help formulate and implement the cybersecurity governance framework, resilience strategy, and education and awareness campaigns. Although the establishment of the CSIRT to be hosted at the DWS requires no development of new legislation and/or policies or amendments of existing ones, the authors recommend that a sector-specific agency be established. This would indeed require either the development of a new piece of legislation or amendment of the CIPA and probably the National Water Act. The rationale behind this recommendation is based on international best practices where it would appear that sector-specific agencies for each classified critical infrastructure sector are the best way to look after the cybersecurity requirements of a sector.
- *Develop a sector cybersecurity governance framework*. Probably most of the sector stakeholders have a cybersecurity governance framework at organisational level based largely, if not solely, on corporate IT security requirements. Such stakeholders merely need to align these with the NCPF as stipulated in Section 16.7 of the policy and incorporate ICS cybersecurity requirements where applicable. At sector level, a governance framework would help with facilitating the exchange of cybersecurity information, sharing of knowledge and collaboration, skills development, and rapid responses to incidents.
- *Develop a sector cybersecurity resilience strategy*. Cybersecurity resilience refers to a critical infrastructure's capability to anticipate, withstand, adapt and/or rapidly recover from any cyber terrorism, cybercriminal activities, cyber vandalism, cyber sabotage, accidents, or naturally occurring threats or human error induced infrastructure failure. This refers more to the water and wastewater ICS as critical infrastructure. Likewise,

at sector level, a cybersecurity resilience strategy would help with ICS cybersecurity information exchange, knowledge sharing and collaboration, skills development, and rapid recovery from any deliberate cyberattacks, accidents, or naturally occurring threats or incidents.

- *Encourage sector members to have documented ICS cybersecurity policies and procedures*. The water and wastewater sector members who either own and/or operate a critical infrastructure (or water ICS) should be encouraged to have documented ICS cybersecurity policies and procedures separate from the corporate IT security policies and procedures in their security operations centres.
- *Develop a sector cybersecurity education and skills development strategy*. A coordinated skills development programme in collaboration with the Cybersecurity Hub in the DCDT, Cybersecurity Centre in the SSA, and other external stakeholders as stipulated in the NCPF should be initiated through the water CSIRT. The sector can partner with academic institutions such as the University of Johannesburg and ICS vendors to develop a formal but customised ICS cybersecurity training and certification programme. This could bolster the specialist domain of ICS cybersecurity in the country tremendously as IT security already has an established body of knowledge and certification programmes. Ultimately, though, the desired picture is to have a cross-functional team of cybersecurity experts in the CSIRT sector to share their varied domain knowledge and experiences to evaluate and mitigate risk in the sector. Thus, cybersecurity operation centres in member organisations should comprise both IT security and specialist ICS cybersecurity experts where applicable.
- *Develop a sector cybersecurity awareness campaign strategy*. Coordinated sector-wide cybersecurity education and awareness campaigns should become regular occurrences.

## 7. Conclusions

The national cybersecurity strategy is a system mainly comprising stakeholders from the justice, crime prevention, and security cluster of South Africa. However, industry, civil society, and other government entities such as the water and wastewater sector are recognised as important stakeholders in the national cybersecurity system. A systems thinking approach was employed to analyse the national cybersecurity and water and wastewater systems. Through the stated stakeholders (system elements/actors) and legislation and policies (system interconnections), the ultimate purpose (system function) of the national cybersecurity system was found to be the establishment of a conducive environment and the provision of guidelines, standards, and best-practices for key cybersecurity stakeholders in South Africa. The interconnected relationships among these key stakeholders were found to be determined largely by the Cybercrimes Bill, CIPA, ECT Act, NCPF, POPI Act, RICA and PAIA in particular, and other cybersecurity-relevant pieces of legislation and policies.

It is concluded that the water and wastewater sector can immediately address its cybersecurity requirements without the need to propose any new legislation and/or government policies or amend existing ones. The aim of the study has therefore been achieved. But the water and wastewater sector will need to identify where changes and concomitant actions in the underlying structure of the national cybersecurity system can result in significant and lasting improvements for the sector. This can only be achieved by establishing a sector CSIRT that should continuously monitor the changes in the underlying structure of the national cybersecurity programme. This is especially important as changing cybersecurity-relevant legislation and policies greatly impact the entire national cybersecurity system, including the water and wastewater sector's cybersecurity responsibilities.

Future research work could use systems thinking or system dynamics to analyse the impact of the national cybersecurity legislation and policies in South Africa since 2015. Other research projects could explore the recommendations discussed above. Moreover, a review of how other countries deal with cybersecurity in the water and wastewater sector in contrast to South Africa should form part of future research works. After all,

the exchange of international experiences is crucial in the advancement of cybersecurity practices. As the country embarks on a digital transformation strategy future research could look at related challenges in the water and wastewater sector. For example, noting that some municipalities have already embarked upon installing smart meters, legislation and policies governing security and privacy of smart water meters and other Internet of Things (smart) devices could be explored.

**Author Contributions:** Conceptualization, All authors; methodology, M.M.; writing—original draft preparation, M.M.; review, A.L.M. and S.v.S.; visualization, M.M.; supervision, A.L.M.; project administration, A.L.M.; funding acquisition, All authors. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Water Research Commission (WRC) of South Africa, grant number 2021/2023-00354, and the article processing charge was also funded by WRC.

**Institutional Review Board Statement:** Not applicable for studies not involving humans or animals.

**Informed Consent Statement:** Not applicable for studies not involving humans or animals.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A Analysis of the National Cybersecurity Policy Framework System

A literature review of the previous analysis work on the National Cybersecurity Policy Framework (NCPF) was conducted in this appendix. This looked at mainly the stakeholders involved, legislation and policies underpinning the national cybersecurity strategy, and challenges in the implementation of the NCPF.

| Researcher | Stakeholders (Elements/Actors) | Legislation and Policies (Interconnections) | Gaps or Identified Challenges |
|---|---|---|---|
| [100] | Domestic<br>• Cybersecurity centre (SSA)<br>• Cyber Crime Centre (SAPS)<br>• Cybersecurity Hub (Department of Telecommunications and Postal Services)<br>• Cyber Command (DoD) | | |
| [101] | Foreign<br>• International Telecommunication Union (ITU) | • NCPF | |
| [102] | Foreign<br>• African Union (AU) | • African Union Convention on Cybersecurity and Personal Data Protection | |

| Researcher | Stakeholders (Elements/Actors) | Legislation and Policies (Interconnections) | Gaps or Identified Challenges |
| --- | --- | --- | --- |
| [36] | Domestic<br>• Justice, crime prevention and security (JCPS) cluster (SSA and others)<br>• Cybersecurity Response Committee (CRC)<br>• Department of Telecommunications and Postal Services (DTPS)<br>• SITA<br>• Department of Science and Technology<br>• Department of International Relations and Cooperation (DIRCO)<br>• South African Revenue Service (SARS)<br>Foreign<br>• International Criminal Police Organisation (Interpol) | • Constitution of the Republic of South Africa<br>• Computer Evidence Act 57 of 1983<br>• Copyright Act 98 of 1978<br>• Critical Infrastructure Bill of 2017<br>• Cybercrimes and Cybersecurity Bill of 2017<br>• ECT Act 25 of 2002<br>• Electronic Communications Act 36 of 2005<br>• Films and Publications Act 65 of 1996<br>• Financial Intelligence Centre Act (FICA) 38 of 2001<br>• National Prosecutions Act 32 of 1998<br>• Monitoring and Prohibition Act 127 of 1992<br>• Prevention of Organised Crime Act 38 of 1999<br>• Promotion of Access to Information Act (PAIA) 25 of 2002<br>• Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004<br>• Protection of Personal Information (POPI) Act 4 of 2013<br>• RICA 70 of 2002 | • New laws and institutions are required in South Africa to effectively address cybersecurity requirements.<br>• The military, intelligence agencies, and critical infrastructure experience the most cyber incidents in South Africa. It should, however, be noted that national critical infrastructure is mostly operated and managed by provincial and local governments as well as the private sector.<br>• New cybersecurity capabilities have to be developed and acquired by South Africa. |
| [66] | Domestic<br>• South African National Defence Force (SANDF)<br>• JCPS cluster | • NCPF<br>• Defence Review<br>• Cybercrimes and Cybersecurity Bill | |

| Researcher | Stakeholders (Elements/Actors) | Legislation and Policies (Interconnections) | Gaps or Identified Challenges |
|---|---|---|---|
| [38] | Domestic<br>• Department of State Security<br>• SSA<br>• SSA Cybersecurity Centre<br>• Electronic Communications Security—Cyber Security Incidents Response Team (ECS-CSIRT)<br>• Department of Justice and Constitutional Development<br>• NPA<br>• SAPS<br>• DoD<br>• Cyberwarfare Command<br>• Centre Headquarters (HQ)<br>• COMSEC Ltd.<br>• Department of Telecommunications and Postal Services<br>• National Cybersecurity Advisory Council<br>• National Cybersecurity Hub<br>• Cyber Inspectorate<br>• Department of Trade and Industry<br>• Public Service and Administration<br>• SITA<br>• Foreign<br>• Forum for Incident Response and Security Teams (FIRST) | • Section 198 of the 1996 Constitution<br>• NCPF<br>• RICA 70 of 2002<br>• Protection of State Information Bill<br>• POPI Act 4 of 2013<br>• Cybercrimes and Cybersecurity Bill<br>• Cyber Warfare Strategy<br>• ECT Act 25 of 2002<br>• Cryptography Regulations<br>• E-government strategy and roadmap<br>• Companies Act 71 of 2008<br>• PAIA 2 of 2000<br>• Corporate Governance of ICT Framework<br>• E-government strategy for each province | • Establishment of a Cyber Inspectorate is provided for in Chapter 12 of the ECT Act. Its mandate includes the powers to inspect, search and seize electronic content in pursuit of illegal activities. However, no regulations were ever promulgated to establish this unit.<br>• Coordination in government is generally an issue. Add to that the inadequacy of existing cybercrime and cybersecurity legal framework, and there is an even bigger issue. The National Cybersecurity Advisory Council was tasked with reducing these deficiencies but there is very little evidence of its activities.<br>• The proposed coordination mechanisms in the NCPF are complex, thus making their management difficult. This is exacerbated by a poor track record of inter-ministerial coordination of programmes. Additionally, there are only limited review and oversight mechanisms, and many activities are shrouded in secrecy.<br>• One of the major challenges for the South African government is the promotion of cybersecurity measures to the (i) national, provincial, and local governments; (ii) general public; (iii) private sector; (iv) civil society; and (v) special interest groups. |

| Researcher | Stakeholders (Elements/Actors) | Legislation and Policies (Interconnections) | Gaps or Identified Challenges |
| --- | --- | --- | --- |
| [103] | Domestic<br>• SSA | • NCPF<br>• ECT Act 25 of 2002<br>• RICA 70 of 2002<br>• POPI 4 of 2013<br>• Cybercrimes and Cybersecurity Bill | |
| [57] | | • NCPF<br>• National Key Points Act 102 of 1980<br>• ECT Act 25 of 2002<br>• King III Report on Corporate Governance | |
| [63] | Domestic<br>• Department of Communications<br>• National Cybersecurity Advisory Council (NCAC)<br>*Foreign*<br>• Council of Europe (CoE) | • NCPF<br>• CoE's Cybercrime Convention | • South Africa was ranked in the top 10 countries most affected by internet crimes. The statistics were drawn from the Internet Crime Complaint Center that is managed by the USA's Federal Bureau of Investigation. The challenge is not a lack of cybercrime laws but enforcing them. There is a huge gap between enacted laws and practical enforcement capability on the ground in most emerging and developing countries such as SA. |

| Researcher | Stakeholders (Elements/Actors) | Legislation and Policies (Interconnections) | Gaps or Identified Challenges |
|---|---|---|---|
| [37] | Domestic<br>• State Security Agency (SSA)<br>• South African Policy Service (SAPS)<br>• Department of Justice and Constitutional Development (DOJ & CD)<br>• National Prosecuting Authority (NPA)<br>• Department of Communications (DOC)<br>• Department of Defence and Military Veterans (DoD & MV)<br>• Department of Science and Technology (DST)<br>• Foreign<br>• African Union<br>• Southern African Development Community (SADC)<br>• Commonwealth | • Films and Publication Act 65 of 1996<br>• Protection from Harassment Act 17 of 2011<br>• Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) 70 of 2002<br>• Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000<br>• Copyright Act 98 of 1978<br>• Consumer Protection Act 68 of 2008<br>• National Archives and Record Service of South Africa Act 43 of 1996<br>• Trade Marks Act 194 of 1993<br>• Designs Act 195 of 1993<br>• Electronic Communications Act 36 of 2005<br>• Electronic Communications and Transactions Act 25 of 2002 (ECT Act)<br>• Independent Communications Authority of South Africa (ICASA) Act 13 of 2000<br>• Inter-Governmental Relations Framework of 2005<br>• Competition Act 89 of 1998<br>• Broadband Infraco Act 33 of 2007<br>• State Information Technology Agency (SITA) Act 88 of 1998<br>• Public Service Act: Regulation | • South Africa follows several global methods. However, a clear commitment towards existing conventions such as the Budapest, AU, SADC and Commonwealth conventions is still outstanding.<br>• Advanced cybersecurity strategies include protection of critical infrastructure (CI) as a key element. The ECT Act also alludes to the protection of CI. However, the implementation of CI protection is still in abeyance. The country had planned for CI protection of the following priority sectors: (i) energy; (ii) information and communications technology; and (iii) transport.<br>• Sector CSIRTs have not yet been established. These would be effective for incident responses and information exchange between sectors.<br>• In the current configuration, the cybersecurity and cybercrime legal framework is spread among very different pieces of legislation. Aligning these would improve predictability and transparency of the policies.<br>• There is a lack of technical cybersecurity skills in government to enable the Cybersecurity Hub to assume the role of a national CERT. Skills development must be prioritised by government in this regard.<br>• A lack of user cybersecurity education and awareness in the general public exacerbates spoofing and phishing related cybercrimes as these are not generally associated with inadequate technical safeguards.<br>• Implementation of a national cybersecurity programme requires sound expertise in several disciplines, and this is lacking in government. This includes commitment and guidance from the top echelons of government, availability and development of the required cybersecurity expert level, and continuous cybersecurity awareness campaigns for the general public. |

| Researcher | Stakeholders (Elements/Actors) | Legislation and Policies (Interconnections) | Gaps or Identified Challenges |
|---|---|---|---|
| [104] | | • NCPF | • In South Africa, cybersecurity awareness initiatives are rolled out through a variety of independent and uncoordinated mechanisms. An integrated and coordinated approach would be effective. |

## References


1. UN. Make the SDGs a Reality. Available online: https://web.archive.org/web/20201110154701/https://sdgs.un.org/#goal_section (accessed on 10 November 2020).
2. White, R. Risk analysis for critical infrastructure protection. In *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*; Gritzalis, D., Theocharidou, M., Stergiopoulos, G., Eds.; Springer: Cham, Switzerland, 2019; pp. 35–54.
3. Birkett, D.; Mala-Jetmarova, H. Plan, prepare and safeguard: Water critical infrastructure protection in Australia. In *Securing Water and Wastewater Systems: Protecting Critical Infrastructure*; Clark, R.M., Hakim, S., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 287–313.
4. Zabašta, A.; Juhna, T.; Tihomirova, K.; Rubulis, J.; Ribickis, L. Latvian practices for protecting water and wastewater infrastructure. In *Securing Water and Wastewater Systems: Protecting Critical Infrastructure*; Clark, R.M., Hakim, S., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 315–342.
5. Möderl, M.; Rauch, W.; Achleitner, S.; Lukas, A.; Mayr, E.; Neunteufel, R.; Perfler, R.; Neuhold, C.; Godina, R.; Wiesenegger, H.; et al. Austrian activities in protecting critical water infrastructure. In *Securing Water and Wastewater Systems: Protecting Critical Infrastructure*; Clark, R.M., Hakim, S., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 343–373.
6. Tiirmaa-Klaar, H. Building national cyber resilience and protecting critical information infrastructure. *J. Cyber Policy* **2016**, *1*, 94–106. [CrossRef]
7. Alexander, A.; Graham, P.; Jackson, E.; Johnson, B.; Williams, T.; Park, J. An analysis of cybersecurity legislation and policy creation on the state level. In *National Cyber Summit (NCS) Research Track. NCS 2019. Advances in Intelligent Systems and Computing*; Choo, K.K., Morris, T., Peterson, G., Eds.; Springer: Cham, Switzerland, 2020; Volume 1055, pp. 30–43.
8. Burmeister, O.; Phahlamohlaka, J.; Al-Saggaf, Y. Good governance and virtue in South Africa's cyber security policy implementation. *Int. J. Cyber Warf. Terror.* **2015**, *5*, 19–29. [CrossRef]
9. Jansen van Vuuren, J.; Leenen, J.; Zaaiman, J.J. Using an ontology as a model for the implementation of the national cybersecurity policy framework for South Africa. In Proceedings of the 9th International Conference on Cyber Warfare and Security 2014 (ICCWS 2014), West Lafayette, IN, USA, 24–25 March 2014; pp. 107–115.
10. Ismail, S.; Sitnikova, E.; Slay, J. Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures: A pilot study. In Proceedings of the 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2014), Xiamen, China, 19–21 August 2014; pp. 1000–1006.
11. NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Available online: https://web.archive.org/web/20201109030328/https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 10 November 2020).
12. Rasekh, A.; Hassanzadeh, A.; Mulchandani, S.; Modi, S.; Banks, M.K. Smart water networks and cyber security. *J. Water Resour. Plan. Manag.* **2016**, *142*, 1–3. [CrossRef]
13. Hassanzadeh, A.; Rasekh, A.; Galelli, S.; Aghashahi, M.; Taormina, R.; Ostfeld, A.; Banks, M.K. A review of cybersecurity incidents in the water sector. *J. Environ. Eng.* **2020**, *146*, 03120003. [CrossRef]
14. Hahn, A. Operational technology and information technology in industrial control systems. In *Cyber-Security of SCADA and Other Industrial Control Systems: Advances in Information Security*; Colbert, E.J.M., Kott, A., Eds.; Springer International Publishing: Cham, Switzerland, 2016; Volume 66, pp. 51–68.
15. Sullivan, D.; Luiijf, E.; Colbert, E.J.M. Components of industrial control systems. In *Cyber-Security of SCADA and Other Industrial Control Systems: Advances in Information Security*; Colbert, E.J.M., Kott, A., Eds.; Springer International Publishing: Cham, Switzerland, 2016; Volume 66, pp. 15–28.
16. Weiss, J. Industrial Control System (ICS) cyber security for water and wastewater systems. In *Securing Water and Wastewater Systems: Protecting Critical Infrastructure*; Clark, R.M., Hakim, S., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 87–105.
17. White, R.; George, R.; Boult, T.; Chow, C.E. Apples to apples: RAMCAP and emerging threats to lifeline infrastructure. *Homel. Secur. Aff.* **2016**, *12*, 1–20.
18. Ramotsoela, D.; Abu-Mahfouz, A.; Hancke, G. A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study. *Sensors* **2018**, *18*, 2491. [CrossRef] [PubMed]

19. Purvis, B.; Mao, Y.; Robinson, D. Three pillars of sustainability: In search of conceptual origins. *Sustain. Sci.* **2019**, *14*, 681–695. [CrossRef]
20. Clark, R.M.; Panguluri, S.; Nelson, T.D.; Wyman, R.P. Protecting drinking water utilities from cyberthreats. *J. Am. Water Works Assoc.* **2017**, *109*, 50–58. [CrossRef]
21. Barbier, E.B.; Burgess, J.C. The sustainable development goals and the systems approach to sustainability. *Econ. E-J.* **2017**, *11*, 1–22. [CrossRef]
22. Chowdhury, R. *Systems Thinking for Management Consultants: Flexible Systems Management*; Springer International Publishing: Singapore, 2019.
23. Fiksel, J. Systems Thinking. In *Resilient by Design: Creating Businesses that Adapt and Flourish in a Changing World*; Fiksel, J., Ed.; Island Press: Washington, DC, USA, 2015; pp. 35–50.
24. Chung, A.; Dawda, S.; Hussain, A.; Shaikh, S.A.; Carr, M. Cybersecurity: Policy. In *Encyclopedia of Security and Emergency Management*; Shapiro, L., Maras, M.H., Eds.; Springer: Cham, Switzerland, 2019.
25. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.* **2019**, *92*, 178–188. [CrossRef]
26. Brechbühl, H.; Bruce, R.; Dynes, S.; Johnson, M.E.E. Protecting critical information infrastructure: Developing cybersecurity policy. *Inf. Technol. Dev.* **2010**, *16*, 83–91. [CrossRef]
27. OECD. Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. Available online: https://web.archive.org/web/20201017142718/http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (accessed on 10 November 2020).
28. UNECE. Working Party on Regulatory Cooperation and Standardization Policies (WP.6)—Report on the Sectoral Initiative on Cyber Security. 2019. Available online: https://web.archive.org/web/20201217093616/https://undocs.org/pdf?symbol=en%2FECE%2FCTCS%2FWP.6%2F2019%2F9 (accessed on 17 December 2020).
29. Sabillon, R.; Cavaller, V.; Cano, J. National Cyber Security Strategies: Global Trends in Cyberspace. *Int. J. Comput. Sci. Softw. Eng.* **2016**, *5*, 67–81.
30. WMO. Water and Cyber Security—Protection of Critical Water-Related Infrastructure. Available online: https://web.archive.org/web/20201118080434/https://public.wmo.int/en/events/meetings/water-and-cyber-security-protection-of-critical-water-related-infrastructure-online (accessed on 17 December 2020).
31. Dlamini, I.Z.; Taute, B.; Radebe, J. Framework for an African policy towards creating cyber security awareness. In Proceedings of the Southern African Cyber Security Awareness Workshop (SACSAW 2011), Gaborone, Botswana, 12 May 2011; pp. 15–31.
32. Budapest Convention. Convention on Cybercrime, European Treaty Series—No. 185. Available online: https://web.archive.org/web/20200724075610/https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (accessed on 10 November 2020).
33. Clough, J. A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation. *Monash Univ. Law Rev.* **2014**, *40*, 698–736.
34. Wicki-Birchler, D. The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? *Int. Cybersecur. Law Rev.* **2020**, *1*, 63–72. [CrossRef]
35. Budapest Convention. Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime, Status as of 05/11/2020. Available online: https://web.archive.org/web/20201110182746/https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=9UQ3WQaH (accessed on 10 November 2020).
36. Ntsaluba, N. Cybersecurity Policy and Legislation in South Africa. Master's Thesis, University of Pretoria, Pretoria, South Africa, 2017.
37. Detecon. E-Commerce, Cybercrime and Cybersecurity—Status, Gaps and the Road Ahead. Available online: https://web.archive.org/web/20201110182612/https://www.dtps.gov.za/index.php?option=com_phocadownload&view=category&download=121%3A20131126_policy-review_e-commerce-cybercrime-and-cybersecurity_final&id=39%3Ae-commerce-cyber-security&Itemid=143 (accessed on 10 November 2020).
38. Sutherland, E. Governance of cybersecurity-the case of South Africa. *Afr. J. Inf. Commun.* **2017**, *20*, 83–112. [CrossRef]
39. Coleman, D. Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Mich. J. Race Law* **2019**, *24*, 417–439.
40. AU Convention. List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection. Available online: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed on 5 November 2020).
41. UN. Resolution Adopted by the General Assembly on 23 December 2015. Available online: https://web.archive.org/web/20200913145346/https://undocs.org/en/A/RES/70/237 (accessed on 10 November 2020).
42. WSIS. Basic Information: About WSIS. Available online: https://web.archive.org/web/20201110172646/https://www.itu.int/net/wsis/basic/about.html (accessed on 10 November 2020).
43. UN. Open-Ended Working Group. Available online: https://web.archive.org/web/20201110172949/https://www.un.org/disarmament/open-ended-working-group/ (accessed on 10 November 2020).

44. UN. Group of Governmental Experts. Available online: https://web.archive.org/web/20201110173326/https://www.un.org/disarmament/group-of-governmental-experts/ (accessed on 10 November 2020).
45. Janke, R.; Tryby, M.; Clark, R.M. Protecting water supply critical infrastructure: An overview. In *Securing Water and Wastewater Systems: Protecting Critical Infrastructure*; Clark, R.M., Hakim, S.S., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 29–85.
46. Clark, R.M.; Hakim, S. *Securing Water and Wastewater Systems: Global Experiences*; Springer International Publishing: Cham, Switzerland, 2014.
47. Spathoulas, G.; Katsikas, S. Towards a secure Industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things: Advanced Sciences and Technologies for Security Applications*; Alcaraz, C., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 29–45.
48. CISA. Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. Available online: https://web.archive.org/web/20201218004033/https://us-cert.cisa.gov/ncas/alerts/aa20-352a (accessed on 18 December 2020).
49. Galinec, D.; Možnik, D.; Guberina, B. Cybersecurity and cyber defence: National level strategic approach. *Automatika* **2017**, *58*, 273–286. [CrossRef]
50. Birkett, D.M. Water critical infrastructure security and its dependencies. *J. Terror. Res.* **2017**, *8*, 1–21. [CrossRef]
51. Chung, J.J. Critical infrastructure, cybersecurity, and market failure. *Or. Law Rev.* **2018**, *96*, 441–476.
52. Bernieri, G.; Pascucci, F. Improving Security in Industrial Internet of Things: A Distributed Intrusion Detection Methodology. In *Security and Privacy Trends in the Industrial Internet of Things: Advanced Sciences and Technologies for Security Applications*; Alcaraz, C., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 161–179.
53. Krotofil, M.; Kursawe, K.; Gollmann, D. Securing industrial control systems. In *Security and Privacy Trends in the Industrial Internet of Things: Advanced Sciences and Technologies for Security Applications*; Alcaraz, C., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 3–26.
54. Clark, R.M.; Hakim, S.; Panguluri, S. Protecting water and wastewater utilities from cyber-physical threats. *Water Environ. J.* **2018**, *32*, 384–391. [CrossRef]
55. Ranathunga, D.; Roughan, M.; Nguyen, H.; Kernick, P.; Falkner, N. Case Studies of SCADA firewall configurations and the implications for best practices. *IEEE Trans. Netw. Serv. Manag.* **2016**, *13*, 871–884. [CrossRef]
56. Panguluri, S.; Phillips, W.; Cusimano, J. Protecting water and wastewater infrastructure from cyber attacks. *Front. Earth Sci.* **2011**, *5*, 406–413. [CrossRef]
57. Pretorius, B.; Van Niekerk, B. Cyber-Security for ICS/SCADA: A South African perspective. *Int. J. Cyber Warf. Terror.* **2016**, *6*, 1–16. [CrossRef]
58. Stellios, I.; Kotzanikolaou, P.; Psarakis, M. Advanced persistent threats and zero-day exploits in industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things: Advanced Sciences and Technologies for Security Applications*; Alcaraz, C., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 47–68.
59. Noble, T.; Manalo, C.; Miller, K.; Ferro, C. Cybersecurity assessments of 30 drinking water utilities. *J. N. Engl. Water Works Assoc.* **2017**, *131*, 219–227.
60. McNabb, J.K. Securing public drinking water utilities. *J. N. Engl. Water Works Assoc.* **2012**, *27*, 37–59.
61. Gourisetti, S.N.G.; Mylrea, M.; Patangia, H. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Gener. Comput. Syst.* **2020**, *105*, 410–431. [CrossRef]
62. Jansen van Vuuren, J.C.; Leenen, L.; Phahlamohlaka, J.; Zaaiman, J. An approach to governance of cybersecurity in South Africa. *Int. J. Cyber Warf. Terror.* **2014**, *2*, 13–27. [CrossRef]
63. Kshetri, N. Cybercrime and cybersecurity issues in the BRICS economies. *J. Glob. Inf. Technol. Manag.* **2015**, *18*, 245–249. [CrossRef]
64. Wolfpack. The South African Cyber Threat Barometer: A Strategic Public-Private Partnership (PPP) Initiative to Combat Cybercrime in SA. Available online: https://web.archive.org/web/20201110174518/http://docplayer.net/17043391-2012-3-the-south-african-cyber-threat-barometer-a-strategic-public-private-partnership-ppp-initiative-to-combat-cybercrime-in-sa.html (accessed on 10 November 2020).
65. South Africa. National Cybersecurity Policy Framework (NCPF). Available online: https://web.archive.org/web/20200701182327/https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed on 10 November 2020).
66. Mutemwa, M.; Mtsweni, J.; Mkhonto, N. Developing a cyber threat intelligence sharing platform for South African organisations. In Proceedings of the Conference on Information Communication Technology and Society (ICTAS 2017), Durban, South Africa, 9–10 March 2017.
67. Government of South Africa. What Are the Government Clusters and Which Are They? Available online: https://web.archive.org/web/20201110180329/https://www.gov.za/faq/guide-government/what-are-government-clusters-and-which-are-they (accessed on 10 November 2020).
68. South Africa. South African Constitution (as amended). Available online: https://web.archive.org/web/20201101003156/https://justice.gov.za/legislation/constitution/SAConstitution-web-eng.pdf (accessed on 10 November 2020).
69. South Africa. Cybercrimes Bill (B6-2017). Available online: https://web.archive.org/web/20200805080827/https://pmg.org.za/bill/684/?via=homepage-card (accessed on 10 November 2020).

70. South Africa. Critical Infrastructure Protection Act 8 of 2019. Available online: https://web.archive.org/web/20201110181412/https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf (accessed on 10 November 2020).
71. South Africa. Protection of Personal Information Act. 2013. Available online: https://web.archive.org/web/20201014062057/https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf (accessed on 10 November 2020).
72. South Africa. The Regulation of Interception of Communications and Provision of Communication-Related Information Act. Available online: https://web.archive.org/web/20200918041001/https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13 (accessed on 10 November 2020).
73. South Africa. Electronic Communications and Transactions Act. Available online: https://web.archive.org/web/20201106144645/https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf (accessed on 10 November 2020).
74. South Africa. Promotion of Access to Information Act No. 2 of 2000. Available online: https://web.archive.org/web/20200517051020/https://www.justice.gov.za/legislation/acts/2000-002.pdf (accessed on 10 November 2020).
75. Karabacak, B.; Yildirim, S.O.; Baykal, N. Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Comput. Law Secur. Rev.* **2016**, *32*, 526–539. [CrossRef]
76. De Bruijn, H.; Janssen, M. Building cybersecurity awareness: The need for evidence-based framing strategies. *Gov. Inf. Q.* **2017**, *34*, 1–7. [CrossRef]
77. DWS. Department of Water and Sanitation 2018/19 Annual Report, Vote 36: Water Is Life—Sanitation Is Dignity. Available online: https://web.archive.org/web/20201110183936/http://www.dwa.gov.za/documents/AnnualReports/19213_Annual%20Report%20201819inhouse.pdf (accessed on 10 November 2020).
78. Government SA. National Water and Sanitation Master Plan, Volume 1: Call to Action, Version 10.1: Ready for the Future and Ahead of the Curve. Available online: https://web.archive.org/web/20200408080543/https://www.gov.za/sites/default/files/gcis_document/201911/national-water-and-sanitation-master-plandf.pdf (accessed on 10 November 2020).
79. Makaya, E.; Rohse, M.; Day, R.; Vogel, C.; Mehta, L.; McEwen, L.; Rangecroft, S.; Van Loon, A.F.E. Water governance challenges in rural South Africa: Exploring institutional coordination in drought management. *Water policy* **2020**, *22*, 519–540. [CrossRef]
80. Government SA. Water and Sanitation. Available online: https://www.gov.za/about-sa/water-affairs (accessed on 10 November 2020).
81. SERI. Water and Sanitation Legislation and Regulations. Available online: https://web.archive.org/web/20170301051254/https://www.seri-sa.org/index.php/links/policy-and-legislation/15-links/policy-and-legislation/87-water-and-sanitation (accessed on 10 November 2020).
82. Stuart-Hill, S.I.; Schulze, R.E. Does South Africa's water law and policy allow for climate change adaptation? *Clim. Dev.* **2010**, *2*, 128–144. [CrossRef]
83. Pedrosa, V.A. The necessity of IWRM: The case of San Francisco river water conflicts. In *Integrated Water Resource Management*; Vieira, E.O., Sandoval-Solis, S., Pedrosa, V.A., Ortiz-Partida, J.P., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 27–34.
84. Meadows, D. *Thinking in Systems: A Primer*; Earthscan: London, UK, 2008.
85. Senge, P.M. *The Fifth Discipline: The Art and Practice of the Learning Organization*; Doubleday, Random House: New York, NY, USA, 2006.
86. Ramos, H. Creativity and Systems Thinking. In *Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship*; Carayannis, E.G., Ed.; Springer International Publishing: New York, NY, USA, 2013; pp. 12–58.
87. Schuster, S. *The art of Thinking in Systems: Improve Your Logic, Think More Critically, and Use Proven Systems to Solve Your Problems*; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 2018; ISBN 9781983847547.
88. SEBoK Editorial Board. *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*; v. 2.3; BKCASE: Hoboken, NJ, USA, 2020.
89. Stroh, D.P. *Systems Thinking for Social Change: A practical Guide for Solving Complex Problems, Avoiding Unintended Consequences, and Achieving Lasting Results*; Chelsea Green Publishing: White River Junction, VT, USA, 2015.
90. Sterman, J.D. *Business Dynamics: Systems Thinking and Modeling for a Complex World*; Irwin/McGraw-Hill: New York, NY, USA, 2000; ISBN 13 9780072311358.
91. Sutherland, E. The Fourth Industrial Revolution–The Case of South Africa. *Politikon* **2020**, *47*, 233–252. [CrossRef]
92. Gcaza, N. Cybersecurity awareness and education: A necessary parameter for smart communities. In Proceedings of the Twelfth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2018), Dundee, Scotland, 29–31 August 2018; pp. 80–90.
93. Mahlaka, R. Experian Offers Mea Culpa after Massive Data Breach Blunder. Available online: https://web.archive.org/web/20201110190306/https://www.dailymaverick.co.za/article/2020-08-23-experian-offers-mea-culpa-after-massive-data-breach-blunder/ (accessed on 10 November 2020).
94. Merten, M. SAPS Regulations: It's Crucial to Watch Critical Infrastructure Rules to Prevent a Power Grab. Available online: https://web.archive.org/web/20200808183846/https://www.dailymaverick.co.za/article/2020-04-03-saps-regulations-its-crucial-to-watch-critical-infrastructure-rules-to-prevent-a-power-grab/ (accessed on 10 November 2020).
95. Timmers, P. The European Union's cybersecurity industrial policy. *J. Cyber Policy* **2018**, *3*, 363–384. [CrossRef]
96. Flowers, A.; Zeadally, S. US policy on active cyber defense. *J. Homel. Secur. Emerg. Manag.* **2014**, *11*, 289–308. [CrossRef]

97. Van Woensel, L. Systems thinking and assessing cross-policy impacts. In *A Bias Radar for responsible POLICY-MAKING: Foresight-Based Scientific Advice*; Van Woensel, L., Ed.; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 69–84.
98. De Jong, M.D.T.; Neulen, S.; Jansma, S.R. Citizens' intentions to participate in governmental co-creation initiatives: Comparing three co-creation configurations. *Gov. Inf. Q.* **2019**, *36*, 490–500. [CrossRef]
99. Karlsson, F.; Holgersson, J.; Söderström, E.; Hedström, K. Exploring user participation approaches in public e-service development. *Gov. Inf. Q.* **2012**, *29*, 158–168. [CrossRef]
100. Phahlamohlaka, J.; Hefer, J. The Impact of cybercrimes and cybersecurity Bill on South African national cybersecurity: An institutional theory analytic perspective. In Proceedings of the THREAT 2019 Cybersecurity Summit, Johannesburg, South Africa, June 2019; pp. 1–7.
101. De Barros, M.J.Z.; Lazarek, H.; Jennifer, M. Comparative study of cybersecurity policy among South Africa and Mozambique. In Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018), Reading, UK, 8–9 March 2018; pp. 521–529.
102. Dalton, W.; Jansen Van Vuuren, J.; Westcott, J. Building cybersecurity resilience in Africa. In Proceedings of the 12th International Conference on Cyber Warfare and Security (ICCWS 2017), Dayton, OH, USA, 2–3 March 2017; pp. 112–120.
103. Van Niekerk, B. An analysis of cyber-incidents in South Africa. *Afr. J. Inf. Commun.* **2017**, *20*, 113–132. [CrossRef]
104. Dlamini, I.Z.; Modise, M. Cyber security awareness initiatives in South Africa: A synergy approach. In *Case Studies in Information Warfare and Security for Researchers, Teachers and Students*; Warren, M., Ed.; ACPIL: London, UK, 2013; pp. 1–22.