CYBER GOVERNANCE IN THE WATER SECTOR

Volume 1 – Water and sanitation cybersecurity legislative and policy environment

Report to the

WATER RESEARCH COMMISSION

by

MASIKE MALATJI, ANNLIZÉ L. MARNEWICK, SUNÉ VON SOLMS & WIKUS ERASMUS

University of Johannesburg

WRC Report No. 3060/1/22

ISBN 978-0-6392-0363-8

March 2023

Obtainable from

Water Research Commission
Bloukrans Building
Lynnwood Bridge Office Park
4 Daventry Road Lynnwood Manor
PRETORIA

orders@wrc.org.za or download from www.wrc.org.za

This report forms part of a set of four reports from WRC project no. 2021/23-00354. The other reports are:

Cyber Governance in the Water Sector. Volume 2: Cybersecurity governance framework for the water sector of South Africa (WRC Report No. 3060/2/22)
Cyber Governance in the Water Sector. Volume 3: Water sector cybersecurity resilience strategy and assessment (WRC Report No. 3060/3/22)
Cyber Governance in the Water Sector. Volume 4: Education and awareness guidelines (WRC Report No. 3060/4/22)

PROJECT EXECUTIVE SUMMARY

INTRODUCTION

South Africa is a major target for cyberattacks. By extension, its critical infrastructure and especially its essential services relating to water and sanitation are at great risk. These risks include physical as well as cybersecurity risks. The focus of this report, in four volumes, is on the cyber risks due to the interconnectedness of the numerous systems that relay information internally as well as externally to the water sector and its role players over communication networks. Although no credible register of cyber incidents or successful attacks exists in South Africa (SA), it is generally accepted that cyberattacks are also directed at strategic key points of the country, including the water and sanitation critical infrastructure (CI).

The requisite cybersecurity efforts and responses are to be coordinated in a governance regime. Governance provides tools and means to guide the behaviour of individuals and autonomous systems in order to achieve a desired outcome. The desired outcome in this case is to harden the water sector's CI against cyber risks through various means. It is in this spirit that the National Cybersecurity Policy Framework (NCPF) was adopted in SA to provide for the effective coordination of government resources. This was done in conjunction with the private sector and civil society, in the achievement of common cybersecurity objectives in cyberspace. The water sector therefore needs to address the sector-specific cybersecurity risks proactively and effectively within the guidelines of the NCPF.

To achieve this, the water sector should (i) examine its cybersecurity legislative and policy environment within the national context; (ii) develop a sector-specific cybersecurity governance framework; (iii) evaluate the sector's cybersecurity resilience posture; (iv) develop guidelines for cybersecurity skills and awareness required in the sector.

The research project is divided into four volumes to address the above objectives at appropriate levels:

Volume	Title	Level
1	Cyber governance in the water sector: Water and sanitation cybersecurity legislative and policy environment	National level
2	Cyber governance in the water sector: Cybersecurity governance framework for the water sector of South Africa	Sector level

3	Cyber governance in the water sector: Water sector cybersecurity resilience strategy and assessment	Organisational level
4	Cyber governance in the water sector: Education and awareness guidelines	Across all levels

The Volume 1 report is a separate deliverable on the contextualisation of the water sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment of SA. Volume 2 outlines the recommended sector-specific cybersecurity governance framework. Volume 3 reports on the cybersecurity resilience assessment levels of four case studies in the water sector. A CI cybersecurity capability framework to determine the minimum cybersecurity considerations for a resilient utility was developed. Volume 4 contains sector-specific cybersecurity education and awareness guidelines. Figure ES-1 highlights the four volumes as summarised in this final report. The details regarding each section are presented in each published volume.

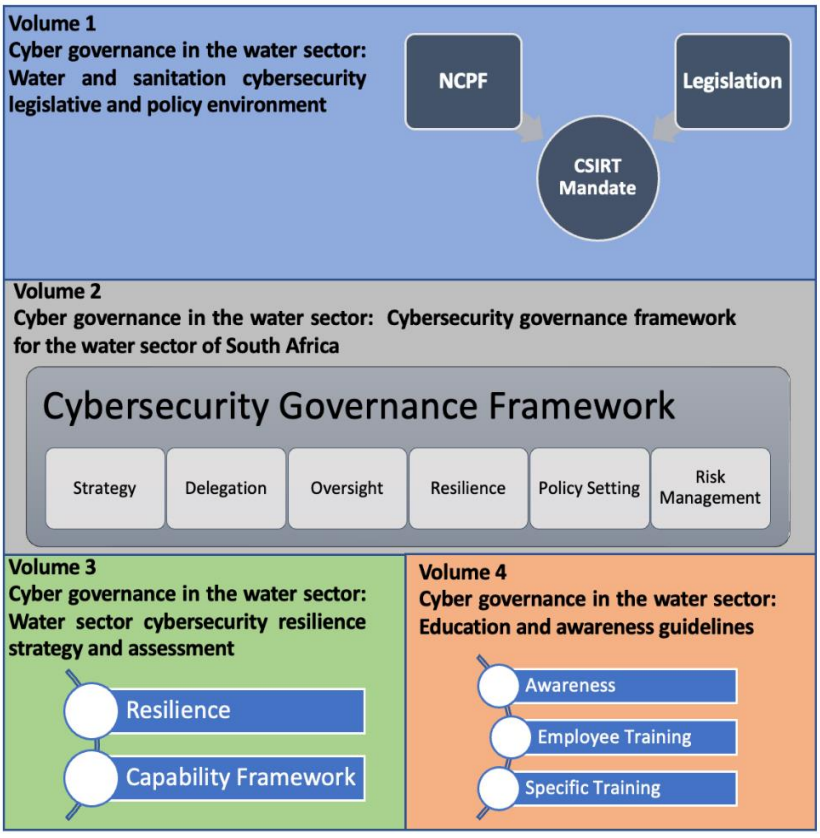

Figure ES-1: Single view of the water sector cyber governance project

The potential value of the output yielded by this research project, including a clear, concise explanation of the extent of the problem and the reasons why the research studies were necessary, are outlined next.

RATIONALE

Extent of the problem. Digital transformation and next-generation technologies have the potential for many benefits in the water sector. Some of these benefits include water utilities' ability to detect leaks in real time and with outstanding accuracy, identify degrading (new and legacy) systems, properly meter water consumption and otherwise make the water value chain more efficient. However, advances in digital technologies can also add to the increased complexity of water CI systems mainly due to the introduction of Internet-based technologies. As alluded to in the WRC project report TT 757/18, this inevitably increases the cyber risk on water CI due to more connectivity. In other words, the introduction of Internet-based technologies multiplies the potential entry nodes of attack on water CIs. It is against this background that a sector-specific cybersecurity governance structure for collective steering and control of cybersecurity practices and human interaction is required. The goal is to safeguard water infrastructure resources proactively and effectively against any cyberattack in a coordinated manner. The purpose is to attain and maintain a high level of cybersecurity resilience in the water sector.

Value of the project outputs. To address the cybersecurity risk effectively and proactively in the water sector of SA, a few fundamentals must be in place. Firstly, a cybersecurity governance structure must be in place to coordinate sector-specific activities with the national cybersecurity bodies. It was established in late 2021 through this research project that the water sector was not represented on the Cybersecurity Response Committee of the Justice, Crime Prevention and Security cluster, the highest national decision-making body pertaining to cybersecurity matters in SA. The Director-General of the Department of Water and Sanitation, through his advisor, was alerted of this finding. In addition, the water sector does not have an existing cybersecurity governance structure as established through research. The value of the project pertaining to this is that a research output proposing the type and mode of the water sector cybersecurity governance structure has been produced.

Secondly, for the water sector cybersecurity governance structure to function optimally, the cybersecurity legislative and policy environment in which it will operate must be understood. The value of the project pertaining to this is that a research output contextualising the water sector's cybersecurity responsibilities within the national cybersecurity legislative and policy framework of SA has been produced. Thirdly, a capable workforce with appropriate cybersecurity skills and knowledge suited for the water sector's mission is required inside and outside the sector-specific cybersecurity governance structure. Research output pertaining to the sector-specific cybersecurity education and awareness campaign materials has been produced.

Lastly, for the water sector cybersecurity governance structure to have an informed baseline from which to start the sector-specific cybersecurity function, the sector cybersecurity resilience level must be measured. This will help determine the sector's ability to anticipate, withstand, adapt and/or rapidly recover from any deliberate cyberattacks, accidents, or naturally occurring threats or incidents. A research output pertaining to the water sector's current cybersecurity resilience level has been produced. Moreover, three tools have been developed in this regard to help the sector attain and maintain a high level of cybersecurity resilience.

Why the project was necessary. In addition to the above, this project was necessary to develop research-based cybersecurity knowledge to benefit the water sector in human capital development, improve top-level decision making through capacity building, reduce the cost of capital through cybersecurity resilience and enable better strategic planning that contributes to the national cybersecurity agenda as envisaged through the NCPF.

AIM AND OBJECTIVES

Project number C2021-2023-0054 has an overarching aim: to develop guidelines on how to manage cybersecurity in the water sector within the national context in which the sector is operating. This is then divided into four specific study aims:

- *Aim 1*. To contextualise the water and sanitation sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment of SA.
    - Objective 1. Identify international and regional cybersecurity policy instruments to perform a high-level benchmarking of SA's policy environment against international practices.
    - Objective 2. Review SA's national cybersecurity legislative and policy environment to determine whether and how other industry and public sectors' cybersecurity responsibilities fit in, to benchmark this against international practices and to determine policy implementation deficits.
    - Objective 3. Review the water and sanitation sector's legislative and policy environment in relation to the national cybersecurity legislative and policy environment to determine whether the sector's cybersecurity responsibilities require amendments to existing laws or enactment of new ones.

- *Aim 2*. To develop a sector-specific cybersecurity governance framework for the water sector of SA.
    - Objective 1. Establish the cybersecurity considerations of the water sector of SA.
    - Objective 2. Develop a suitable water sector cybersecurity governance framework with a clear governing body, governance structure and mode.
- *Aim 3*. To develop and evaluate the cybersecurity resilience levels of SA's water sector.
    - Objective 1. Develop a socio-technical systems cybersecurity resilience assessment model.
    - Objective 2. Evaluate the South African water sector cybersecurity resilience level.
- *Aim 4*. To provide cybersecurity education and awareness campaign materials and guidelines suitable for usage by the water sector of SA.
    - Objective 1. Determine the cybersecurity work roles for the whole sector and all the levels in the sector to which they apply.
    - Objective 2. Determine the baseline knowledge which every employee in the sector should have.
    - Objective 3: Provide guidelines for education and awareness continuous improvements.

METHODOLOGY

In order to achieve the aims of the study, a four-step methodology was employed. Each step corresponds with a respective volume and the full details are discussed in that particular text.

The four steps are as follows:

Step 1: Water and sanitation cybersecurity legislative and policy environment

Aim 1: Contextualise the water and sanitation sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment of SA.

<table>
<tr><td>National level</td><td>Identify the national cybersecurity stakeholders, legislation and policies.</td><td rowspan="3">Water and sanitation cybersecurity legislative and policy environment (Volume 1)</td></tr>
<tr><td>Sector level</td><td>Identify the water sector stakeholders, legislation and policies.</td></tr>
<tr><td colspan="2">Analyse interrelationships between national and sector level.</td></tr>
</table>

Step 2: Cybersecurity governance in South Africa

Aim 2: Develop a sector-specific cybersecurity governance framework for the water sector of SA.

National policy	Input from step 1: Water and sanitation cybersecurity legislative and policy environment	Framework for governance of cybersecurity in the water sector (Volume 2)
Governance best practices	Identify the cybersecurity governance practices.	
Literature case studies	Retrieve lessons learnt from literature case studies.	

Step 3: Cybersecurity resilience levels of SA's water sector

Aim 3: Develop and evaluate the cybersecurity resilience levels of SA's water sector.

Cybersecurity resilience model	Define resilience assessment approach for water organisations.	Cybersecurity capabilities for critical infrastructure resilience
Cybersecurity resilience baseline	Measure four case studies for cybersecurity resilience.	

Step 4: Cybersecurity governance in the water sector – a training guide

Aim 4: Provide cybersecurity education and awareness campaign materials and guidelines suitable for usage by the water sector of SA.

Cybersecurity employee knowledge	Develop and measure cybersecurity awareness. Identify cybersecurity knowledge requirements for water sector employees. Identify cybersecurity knowledge requirements for technical expertise water sector employees.	Education, training and awareness guidelines

Aims and objectives were developed for each volume and corresponding step.

KEY RECOMMENDATIONS

A description is given in each volume of how the respective aims were approached and ultimately achieved in order to provide detailed recommendations. The following key recommendations emerged from the research:

- From Volume 1:

- Establish a water sector Cybersecurity Incident Response Team (CSIRT) that can coordinate efforts in the sector and facilitate interaction to fight cybersecurity incidents and ensure that relevant stakeholders are included at national level.

- From Volume 2:
  - Implement cybersecurity governance practices at sectoral level.
- From Volume 3:
  - Develop organisational capabilities to establish resilience in the cybersecurity context.
  - Develop human resource capabilities through adequate training and maintenance of skills.
- From Volume 4:
  - Develop organisational capabilities to establish resilience in the cybersecurity context.

In essence, the key recommendations will serve to transform the water and sanitation cybersecurity environment. Figure ES-2 demonstrates the state of affairs:

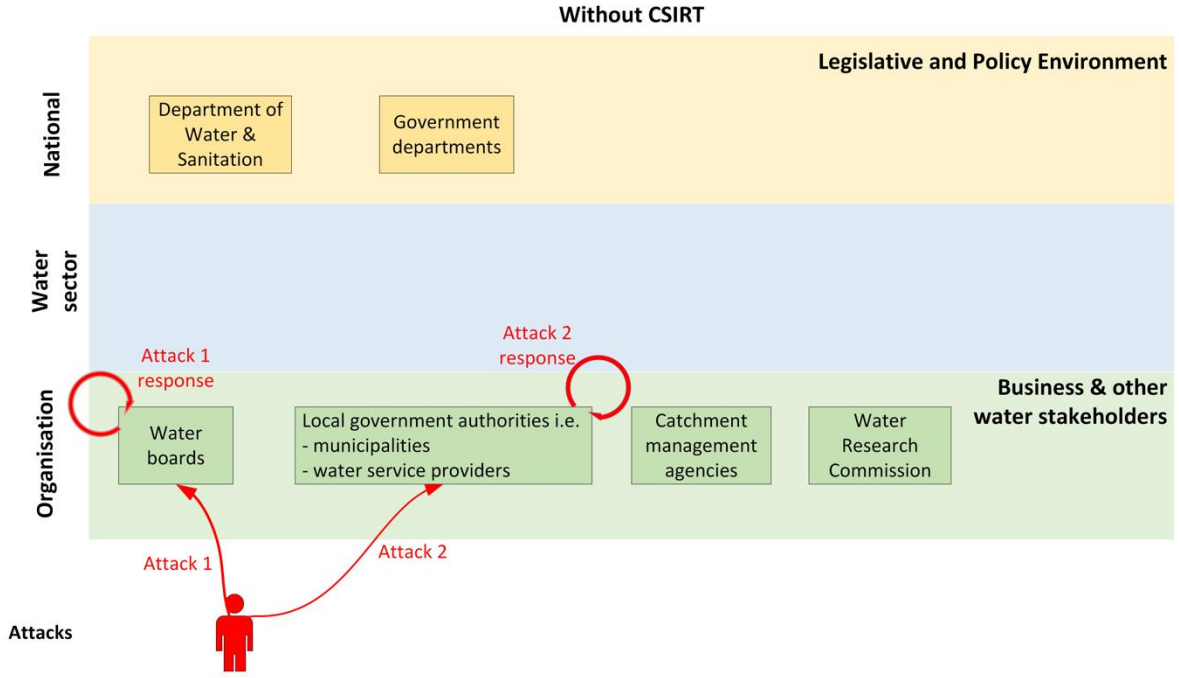

Figure ES-2: Current water and sanitation sector environment without CSIRT

Currently, the three spheres of influence operate in a mostly uncoordinated manner. Vertically, there is little communication or coordination between the national legislative environment, the sectoral level and the implementation level where the organisations responsible for water and

sanitation operations reside. Likewise, this coordination is lacking horizontally where bodies and organisations at the same level find it difficult to coordinate and act on intelligence from current or previous cyber incidents.

What the key recommendations seek to achieve can be depicted in Figure ES-3.

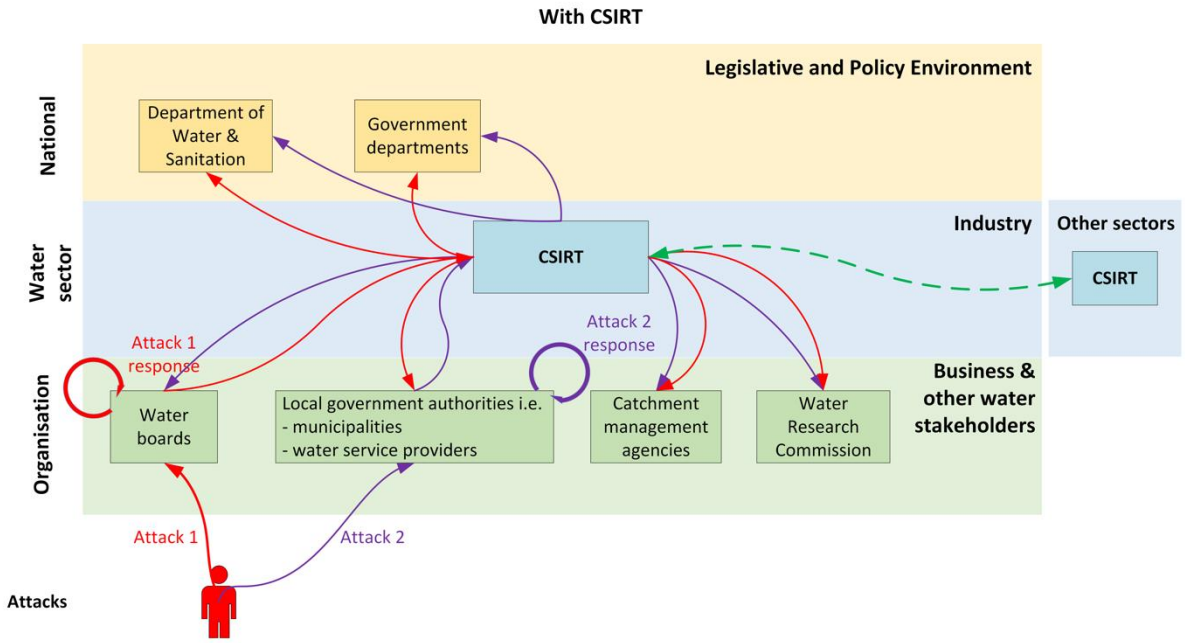

Figure ES-3: Water and sanitation sector with CSIRT

With the adoption of a CSIRT, horizontal and vertical coordination can be achieved. Protocols and procedures are placed in a governance regime so that any and all cyber incidents are reported to the CSIRT to coordinate responses. Firstly, the attacked organisation or body implements immediate response measures as they are trained to in the context of increased resilience. The CSIRT is almost immediately notified in case certain aspects are not directly monitored by the CSIRT. The CSIRT responds by supporting any organisations that are being attacked and uses intelligence to prepare other organisations that are not experiencing a specific attack to either repel or proactively prevent further such attacks. The CSIRT then also reports to other sectoral CSIRTs. This serves to increase horizontal coordination.

Secondly, vertical coordination is improved in the same manner but also by the CSIRT informing national bodies of current and past cyber incidents in order to facilitate a national response. This may serve to hone the national cybersecurity strategy in response to threats experienced and consolidation of data to determine what trends are manifesting.

FUTURE RESEARCH

This body of work has raised some questions that need to be answered in future research as they fall beyond the scope of the aims of the four volumes. The following future projects or avenues for research have been identified:

- Derive a guideline to establish a water CSIRT: Even though a CSIRT is mandated through national policy, there are no guidelines for establishing a CSIRT other than charter elements that it should include. The steps to be considered to establish such a body given the national policy and legislative contexts need to be determined. Additionally, it would be helpful to determine what the risks and pitfalls could be in establishing this body and how to minimise disruption in the sector during such an undertaking. What would be of paramount importance is to ensure that all the relevant stakeholders and resources are identified and represented in this body and to formulate how they would interact at their respective levels.
- Volume 2 focuses on the sectoral implementation of governance practices in the form of a framework. What may benefit from more in-depth investigation is how cybersecurity strategy can be aligned with organisational and implementation level realities. This may require a sample of cybersecurity strategy and implementation audits to be carried out at various water sector bodies to determine the extent of implementation and the value of currently implemented practices. This may provide insight into what cybersecurity governance practices are considered important, where gaps exist and what practices need to be maintained, if not developed further.
- It is evident that there are training needs at the various strategic levels. What can be uncovered in more detail is how these training needs differ and what specialised training must be implemented. This can be applied to specific roles and levels of responsibility. It is conceivable that these needs will diversify depending on the particular water sector body under scrutiny and the level at which the various roles operate. What complicates matters even further is that the threat landscape is much more dynamic than the reactive legislative and policy environment. This forces training to be more responsive to current and near-term future threats.

Each volume focuses on issues specific and pertinent to the aims and objectives set out above. Volume 1 now follows to explore international water and sanitation legislation and policy, which are compared to the South African environment to find gaps and recommendations in this regard.

VOLUME 1: EXECUTIVE SUMMARY

BACKGROUND

A wide range of corporate information technology and operational technology cybersecurity threats and vulnerabilities in the water sector have been identified by both industry and academia. Some are associated with municipal water distribution systems that can easily be sabotaged or even damaged by means of contamination injection, cyberattack or physical destruction (Janke, Tryby & Clark, 2014). In many countries, as in South Africa, critical infrastructure owners have focused largely on physical security. However, with the increased connectivity through digital technologies and communication networks, cybersecurity has become an area of increasing concern. This is also true of the water and sanitation sector as utilities are increasingly using smart or connected industrial control systems for their operational technologies. These are essential for the monitoring and control of physical processes essential to water treatment plants and distribution systems.

It is known that strategic installations of the country, including the water and sanitation critical infrastructure, are being targeted. It is therefore prudent for the sector to holistically examine its cybersecurity risk level, from legislation and policies to governance and capability, and from everyday practices to awareness.

RATIONALE

Although various cybersecurity threats and vulnerabilities have been identified in the water sector, it should be noted that drinking water and wastewater plant operational scenarios differ. Thus, cybersecurity threats and vulnerabilities should be analysed in perspective (Weiss, 2014). This means that the water and sanitation sector must evaluate its specific cybersecurity threats and vulnerabilities, and thereafter employ suitable mitigation strategies (Janke et al., 2014).

This points to the need for adaptive cybersecurity strategies, legislation and policies to provide for appropriate cybersecurity governance of the sector. It is in this spirit that the national cybersecurity policy framework was adopted in South Africa to provide for the effective coordination of departmental resources in achieving common cybersecurity safety and security objectives in cyberspace. The water and sanitation sector therefore needs to address its sector-specific cybersecurity risks proactively and effectively within the guidelines of the national cybersecurity policy framework. Contextualisation of the water and sanitation sector's cybersecurity responsibilities within the national cybersecurity policy and legislative environment is therefore necessary.

AIM AND OBJECTIVES

The aim of the WP1 study was to contextualise the water and sanitation sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment of South Africa. The objectives of the study were as follows:

- Identify international cybersecurity policy instruments in order to perform a high-level benchmarking of South Africa's policy environment against international practices.
- Review South Africa's national cybersecurity legislative and policy environment to determine whether and how other industry and public sectors' cybersecurity responsibilities fit in, to benchmark this against international practices and to determine policy implementation deficits.
- Review the water and sanitation sector's legislative and policy environment in relation to the national cybersecurity legislative and policy environment to determine whether the sector's cybersecurity responsibilities require amendments to existing laws or enactment of new ones.

METHODOLOGY

Considering the complex nature of government policy and the different parties involved in effecting legislation, the systems thinking approach was deemed suitable for contextualising the water and sanitation sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment of South Africa. Four systems thinking steps were executed in this regard:

- Identify the national cybersecurity purpose, stakeholders, legislation and policies.
- Identify the water and wastewater sector's purpose, stakeholders, legislation and policies.
- Identify the water and wastewater sector within the national cybersecurity governance system.
- Analyse (purpose, stakeholders and government policy) interrelationships between the water and wastewater sector and national cybersecurity governance system.

The application of these steps helped identify where and how the water and sanitation sector's cybersecurity requirements can be met, as elaborated on next.

RESULTS AND DISCUSSION

The study results are as follows:

- The cybersecurity stakeholders, legislation and policies of the international cybersecurity system are partially defined, and the cybersecurity purpose is clearly defined.
- The cybersecurity purpose, stakeholders, legislation and policies of the national cybersecurity system are clearly defined.
- The cybersecurity purpose, stakeholders, legislation and policies of the water and wastewater sector as an independent system are not defined.
- The cybersecurity purpose, stakeholders, legislation and policies of the water and wastewater sector as an actor in the national cybersecurity system are clearly defined.

The study found that the water and sanitation sector's cybersecurity purpose, stakeholders, legislation and policies are only clearly defined if the sector is represented by the 'public sector cyber security incidents response teams (CSIRTs)' designation in the national cybersecurity governance system. This means that the cybersecurity roles and responsibilities of the water and sanitation sector require, among other things, that the sector CSIRTs be established to serve the cybersecurity interests of the sector. The water and sanitation sector's CSIRT is expected, in particular, to develop national cybersecurity standards and best practices for the sector in consultation with the Cybersecurity Centre (located in the Ministry of State Security) and the Justice, Crime Prevention and Security Cybersecurity Response Committee. These should be consistent with guidelines, standards and best practices defined in line with the national cybersecurity policy framework.

This finding effectively means that the water and sanitation sector can establish its sector-specific CSIRT with no requirements for new laws and government policy. The main questions, however, are regarding the cybersecurity governance structure of the sector. Where will the CSIRT be hosted? Where will it report to? Is a Department of Water and Sanitation-hosted CSIRT the best governance option to look after the sector's cybersecurity requirements optimally? In addressing these questions and the identified cybersecurity policy implementation deficits, international cybersecurity governance best practices were briefly reviewed.

The full systematic literature review of these will form part of WP2 and WP3 deliverables. However, insight drawn from the brief review indicates that a sector-specific agency dedicated to the cybersecurity role and responsibilities of the sector is a better governance model. This and other policy recommendations are outlined below.

POLICY RECOMMENDATIONS

Two sets of recommendations are made. These concern both the water and sanitation sector and national cybersecurity policy framework. Regarding the water and sanitation sector's cybersecurity responsibilities within the national cybersecurity legislation and policy environment, the following recommendations are made:

- Establish a sector CSIRT. Establish the national water CSIRT that will have specialist teams serving the cybersecurity requirements of both corporate information technology and industrial control systems to help formulate and implement the cybersecurity governance framework, resilience strategy and education and awareness campaigns. Although the establishment of the CSIRT to be presumably hosted at the Ministry of Water and Sanitation requires no development of new legislation and/or policies or amendments to existing ones, the project team recommends that a sector-specific agency be established. This would indeed require either the development of new legislation or an amendment to the Critical Infrastructure Protection Act 8 of 2019 and probably the National Water Act 36 of 1998, and other policies. The rationale for this recommendation is based on international best practices. It would appear that a sector-specific agency for each classified critical infrastructure sector, including the water and sanitation sector, is the best way to efficiently identify, protect, detect, respond and recover from any cybersecurity threats and attacks in the sector. A sector-specific agency provides the most efficient way to coordinate, manage, collaborate and share information on sector incidents, and provide thought leadership and policy recommendations for the sector. The implementation of this recommendation is beyond the scope of the current project.
- *Determine the sector's cybersecurity resilience level. This recommendation will be achieved as part of the WP2 deliverable in the current project.*
- *Develop a sector cybersecurity governance framework. This recommendation will be achieved as part of the WP3 deliverable in the current project.*
- *Encourage sector members to have documented cybersecurity policies and procedures for industrial control systems. This recommendation will be achieved as part of the WP3 and WP4 deliverables in the current project.*
- *Develop a sector cybersecurity education and skills development strategy. This recommendation will be achieved as part of the WP4 deliverable in the current project.*
- *Develop a sector cybersecurity awareness campaign strategy. This recommendation will be achieved as part of the WP4 deliverable in the current project.*

Regarding the national cybersecurity policy framework, several recommendations are made as a result of policy implementation deficits and generally poor track record of interministerial

coordination of programmes. The details of the recommendations are discussed in Chapters 3 and 7 but can be summarised in one sentence. The South African government should reconsider the cybersecurity mandates and operating models of key cybersecurity stakeholders such as the Department of Communications and Digital Technologies and other ministries and public entities.

CONCLUSIONS

The national and water and wastewater sector cybersecurity deficits (gaps and challenges) were identified. It is concluded that the water and wastewater sector can immediately address its cybersecurity requirements to deal with these deficits without the need to propose any new legislation and/or government policies or amend existing ones. This is in order as long as the sector's cybersecurity practices are in line with the guidelines, standards and best practices defined by the Justice, Crime Prevention and Security Cybersecurity Response Committee.

At policy level, the water and wastewater sector's cybersecurity and information and communications technology practices must be in accordance with the national cybersecurity policy framework and supporting legislation. At technical level, including risk management and technological safeguards, a best-practice water utilities cybersecurity governance framework should be developed to facilitate the adequate protection of the sector's critical infrastructure and also address the identified gaps and challenges. This forms part of the next steps to achieve the WP2 and WP3 deliverables.

FUTURE RESEARCH

Although the WRC Report No. TT 757/18 discussed the Internet of Things, it focused only on the applications of this emerging technology in the water and sanitation sector. Future research work could specifically explore the Internet of Things (e.g. smart water meters) cybersecurity and privacy policies in the water and sanitation sector of South Africa considering the POPI Act 4 of 2013 and PAIA 25 of 2002. In the same breath, as the fourth generation of industrial control systems – Industrial Internet of Things – is gradually adopted in the sector globally, cybersecurity risks introduced by such deployments should be researched. A continuous review, through an established sector-specific CSIRT, on how other countries deal with cybersecurity in the water and wastewater sector in contrast to South Africa should also form part of future research works.

The report layout is as follows: The aim and objectives of the first deliverable as well as the study method followed to achieve them are introduced in section 1. Sections 2, 3 and 4 contain reviews of international, national and water sector cybersecurity purpose, stakeholders, policies and legislation, respectively. The results are presented in section 5 and discussed in

section 6. The study recommendations are outlined in section 7 with a conclusion and areas for future research in section 8.

KNOWLEDGE DISSEMINATION

The research conducted under WP1 has led to an international peer-reviewed journal publication. As a result, the content of this report is an outcome of the journal publication as follows:

- Malatji, M., Marnewick, A.L. & Von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability*, 13 (1), 291, pp. 1-33, https://doi.org/10.3390/su13010291.

ACKNOWLEDGEMENTS

The authors would like to thank the following individuals for their input during WRC Project C2021-2023-00354.

Name	Title	Affiliation
Dr Nonhlanhla Kalebaila	Research Manager	Water Research Commission
Ms Charmaine Khanyile	Project Co-ordinator	Water Research Commission
Mr Dumisani Gubuza	Reference group member	City of Tshwane
Ms Kgaogelo Kubyana	Reference group member	eMalahleni municipality
Mr Vusi Kubheka	Reference group member	RandWater
Ms Nomazwi Mhloma	Reference group member	eThekwini Metro municipality
Mr Mluleki Mnguni	Reference group member	Umgeni Water
Mr Moloko Monyepao	Reference group member	Ekurhuleni municipality
Mr Dan Naidoo	Reference group member	Umgeni Water
Dr Kiru Pillay	Reference group member	Department of Communication and Digital Technologies
Dr Renier van Heerden	Reference group member	SANREN
Dr Brett Van Niekerk	Reference group member	Durban University of Technology

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

AU	African Union
BRICS	Brazil, Russia, India, China, South Africa
CIPA	Critical Infrastructure Protection Act
CISA	Cybersecurity and Infrastructure Security Agency
COMSEC	Electronic Communications Security (Pty) Ltd
CRC	Cybersecurity Response Committee
CSIRT	Cyber Security Incidents Response Team
DCDT	Department of Communications and Digital Technologies
DoD	Department of Defence
DWS	Department of Water and Sanitation
ECS-CSIRT	Electronic Communications Security—Cyber Security Incidents Response Team
ECT	Electronic Communications and Transactions
FIRST	Forum of Incident Response and Security Teams
ICS	Industrial Control System
ICT	Information and Communications Technology
IT	Information Technology
JCPS	Justice, Crime Prevention and Security
NCPF	National Cybersecurity Policy Framework
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PAIA	Promotion of Access to Information Act
POPI	Protection of Personal Information
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act
S1, 2, 3	Student one, two, three
SA	South Africa
SABRIC	South African Banking Risk Information Centre
SAPS	South African Police Service
SEBoK	Systems Engineering Body of Knowledge
SERI	Socio-economic Rights Institute
SLR	Systematic literature review
SSA	State Security Agency
STS CF	Socio-technical Systems Cybersecurity Framework

UN	United Nations
UNECE	United Nations Economic Commission for Europe
USA	United States of America
WMO	World Meteorological Organisation
WP	Work package
WRC	Water Research Commission
WSIS	World Summit on the Information Society

1. INTRODUCTION AND OBJECTIVES

1.1 Introduction

The next-generation technologies and digital transformation in critical infrastructure have changed the security focus of many countries to not only physical security, but also cybersecurity as these advances add increased complexity to the critical infrastructure systems. This is also true for the water and sanitation/wastewater[1] sector as utilities are increasingly using smart industrial control systems (ICSs) for their operational technologies on top of the information technology (IT) systems already in place. The water and sanitation sector therefore needs to address the sector-specific cybersecurity risks proactively and effectively.

There is no doubt that individual organisations in the water and sanitation sector have information and communications technology (ICT) policies in place to address IT security and information security requirements. However, there is limited to virtually no literature available on cyber risk governance practices in the South African water and sanitation sector. As noted in the WRC Report No. TT 667/16 of 2016, "*a number of water service authorities and water service providers are thought to be struggling to establish risk governance activities and to integrate them into wider business functions*". This refers to risk management in its pure and generic form. It is no surprise then that the literature on cyber risk governance practices in the water and sanitation sector is virtually non-existent.

Therefore, the development of cyber risk governance practices for the water and sanitation sector has emerged as a key strategic priority in South Africa to manage cybersecurity threats and vulnerabilities in the sector proactively. To do this, the cybersecurity legislative and policy environment must first be understood in order to subsequently develop the appropriate cybersecurity governance framework, resilience strategy and education and training materials. In addition, South Africa's cybersecurity policy instruments as well as critical infrastructure protection practices should be benchmarked against international practices.

In response to this call, the University of Johannesburg's Faculty of Engineering and the Built Environment was commissioned by the Water Research Commission (WRC) to undertake a study entitled 'Cyber governance in the water sector' with four work packages or deliverables. This report is about work package 1 (WP1), which is aimed at contextualising the cybersecurity legislative and policy environment of the water and sanitation sector within the national cybersecurity policy.

[1] The term 'sanitation' is used interchangeably with 'wastewater' in this report. That is, 'water and sanitation' carries the same meaning as 'water and wastewater' throughout the report.

1.2 Project aim and objectives

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 sanitation is one such sector that needs to conduct its own cybersecurity risk assessments and determine its resilience level. In light of this, the aim of WP1's study was to contextualise the water and sanitation sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment of South Africa. The objectives of the study were as follows:

- Identify international cybersecurity policy instruments in order to perform a high-level benchmarking of South Africa's policy environment against international practices.
- Review South Africa's national cybersecurity legislative and policy environment to determine whether and how other industry and public sectors' cybersecurity responsibilities fit in, to benchmark this against international practices and to determine policy implementation deficits.
- Review the water and sanitation sector's legislative and policy environment in relation to the national cybersecurity legislative and policy environment to determine whether the sector's cybersecurity responsibilities require amendments to existing laws or enactment of new ones.

1.3 Project approach

The systems thinking approach (Meadows, 2008; Senge, 2006), complemented by thematic content analysis (Braun & Clarke, 2006; Saunders, Lewis & Thornhill, 2016), was employed primarily to achieve the research aim. This took into consideration the dynamic and complex nature of government policy environments in South Africa. Systems thinking helps to holistically examine dynamic patterns and events by focusing on the interrelations between a system's parts rather than seeing the constituent parts as static, standalone and unrelated elements (Meadows, 2008; Senge, 2006). It is a method to identify and understand how the parts interrelate within the entire system (Ramos, 2013). In this report, a system is perceived as a set of independent but *interconnected* subsystems or *elements/actors* that form an integrated structure to perform a harmonious *function or purpose* (Chowdhury, 2019; Schuster, 2018; Fiksel, 2015; SEBoK Editorial Board, 2016). A system can be visualised as shown in Figure 1.

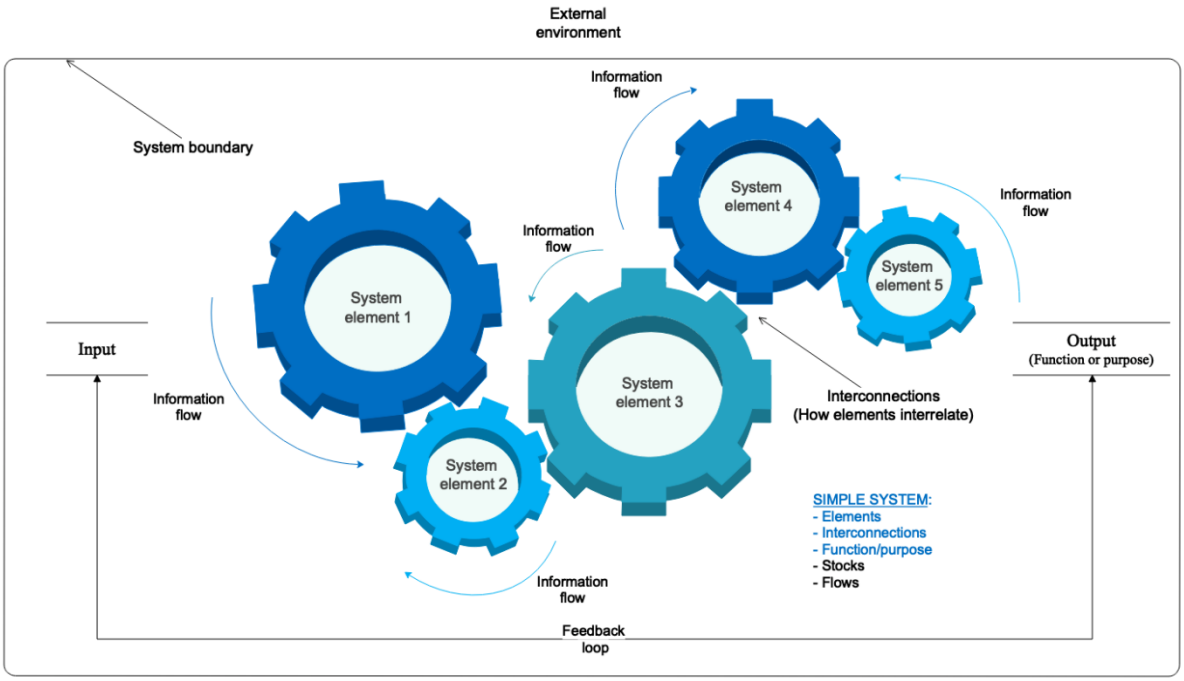

Figure 1. An open system. Adapted from Chowdhury (2019)

For the purpose of this study, a system can thus be considered to comprise the national cybersecurity **stakeholders** as *elements/actors* of the system, national cybersecurity **legislation and policies** as *interconnections* inside and outside the system, and national cybersecurity's **key objectives** as a *function/purpose* of the system. Adapted from Chowdhury (2019), Figure 1 shows a snapshot view of a system – read *open* system (SEBoK Editorial Board, 2016) – with the arrows indicating the inflow and outflow knowledge, information and other intangible activities between and among the stakeholders of a system, as well as the feedback loops that regulate the system to self-correct (Meadows, 2008; Sterman, 2000). The systems thinking approach is one of the best methods to provide an appraisal of policy implementation deficits and impact. To achieve the aim of the study, four systems thinking steps were executed as follows:

- Identify the national cybersecurity system function, actors and interconnections.
- Identify the water and wastewater system function, actors and interconnections.
- Identify the water and wastewater system as an actor in the national cybersecurity system.
- Analyse interrelations between the water and wastewater and national cybersecurity systems.

1.4 Report layout

The structure of this report is as follows:

- Chapter 1 introduces the aim and objectives of the first deliverable (WP1). The study method followed to achieve the aim of the study is also described in this chapter.
- The international cybersecurity policy instruments in order to perform a high-level benchmarking of South Africa's policy environment against international practices are identified in Chapter 2. This is in relation to the first objective of the study.
- Chapter 3 is a review of South Africa's national cybersecurity legislative and policy environment to determine whether and how other industry and public sectors fit in, to benchmark against international practices and to determine policy implementation deficits. This is in relation to the second objective of the study.
- In Chapter 4 the water and sanitation sector's legislative and policy environment is reviewed in relation to the national cybersecurity legislative and policy environment to determine whether the sector's cybersecurity responsibilities require amendments to existing laws or enactment of new ones. This is in relation to the third and final objective of the study.
- Chapter 5 presents the results based on the execution of the four study approach steps described in the previous section.
- The ramifications of the study findings are discussed in Chapter 6, in particular, the cybersecurity policy implementation deficits and whether the water and sanitation sector's cybersecurity responsibilities require amendments to existing laws or enactment of new ones.
- Two policy briefs are outlined in Chapter 7. Firstly, recommendations are made on how the national cybersecurity policy implementation deficits can be improved. Secondly, recommendations are made on how the water and sanitation sector can address its cybersecurity responsibilities.
- Chapter 8 concludes the report and relevant areas are proposed for future research.

2. INTERNATIONAL CYBERSECURITY POLICY ENVIRONMENT AND PRACTICES

2.1 Introduction

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) (2019) and Sabillon, Cavaller and Cano (2016) assert, cyberthreats cut across any social and economic activities nationally, regionally and internationally. It is therefore prudent to explore international cybersecurity cooperation mechanisms available 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.

2.2 International cybersecurity stakeholders

In the Protection of Critical Water-related Infrastructure Cybersecurity Webinar held on 18 November 2020 by the World Meteorological Organisation (WMO, 2020), one of the UNECE speakers indicated that work encouraging common regulatory frameworks in specific sectors with critical impact on sustainable development is underway at the UN. This includes a report on the sectoral initiative on cybersecurity by the UNECE (2019), 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 (Appendix A) and are as follows:

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

The African Network Information Centre is missing in Appendix A and is regarded by Dlamini, Taute and Radebe (2011) as a relevant stakeholder on the African continent regarding security of cyberspace. In the next section some of the available treaties and conventions governing international cybersecurity cooperation and the interrelationships between the stakeholders mentioned above are explored.

2.3 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, is the first international cooperation mechanism on issues relating to cybersecurity and cybercrime (Clough, 2014). It attempts to provide signatory states with a common international policy to fight harmoniously against cybercriminals (Wicki-Birchler, 2020). Of the 47 member states of the Council of Europe, only one—the Russian Federation—has not signed (Budapest Convention, 2020), citing infringement of its (Internet) sovereignty (Ntsaluba, 2017). Ireland and Sweden are the only two member states that have signed but never ratified the Convention (Budapest Convention, 2020). 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 it (Detecon, 2013; Sutherland, 2017). Thus, the total number of signatures not followed by ratifications stood at three—South Africa, Ireland and Sweden—as of 10 November 2020. In addition, the total number of ratifications now stands at 65 (Budapest Convention, 2020). 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 (Clough, 2014). On the African continent, however, the AU adopted the Convention on Cyber Security and Personal Data Protection in June 2014 (Coleman, 2019; Ntsaluba, 2017; Sutherland, 2017). According to Coleman (2019), the AU Convention provides a framework for personal data protection which member countries may transpose into their domestic legislation, but it 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 (AU Convention, 2020). South Africa has not yet signed the AU Convention.

There have 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 (UN, 2015), the World Summit on the Information Society (WSIS) Geneva Plan of Action (WSIS, 2020), Global Cybersecurity Agenda by the International Telecommunication Union (Clough, 2014), the Open-Ended Working Group based on UN General Assembly resolution 73/27 (UN, 2020a) and the Group of Governmental Experts based on UN General Assembly resolution 73/266 (UN, 2020b). South Africa is a member of the Group and, along with 24 other member states, is expected to submit a final report to the UN General Assembly in 2021 (UN, 2020c). In summary, some of the most pertinent international cybersecurity laws are as follows:

- The Budapest Convention
- The International Telecommunication Union 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 is binding as yet. This leaves the Budapest Convention on international cybercrime as the only treaty that is binding on its member states. Clough (2014:725), 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.

2.4 International water-specific cybersecurity challenges

It was mentioned earlier that ICSs are essentially the backbone of critical infrastructure worldwide, including water and wastewater critical infrastructure. The introduction of cyber connectivity into ICS environments has increased the vulnerability of all types of critical infrastructure to cyberattacks (Birkett & Mala-Jetmarova, 2014; Clark & Hakim, 2014; Janke, Tryby & Clark, 2014; Spathoulas & Katsikas, 2019). Recently, the Cybersecurity and Infrastructure Security Agency (CISA) (2020) of the United States of America (USA) has reported compromises of critical infrastructure, government agencies and private sector organisations through a third-party contractor network management tool called SolarWinds Orion platform.

According to CISA (2020), this advanced persistent threat (Galinec, Moznik & Guberina, 2017) began approximately in March 2020, with evidence suggesting that there are additional initial access vectors other than the SolarWinds Orion platform. These threats are cyberattacks carried out repeatedly over an extended period by actors with significant resources and sophisticated levels of expertise (Clark, Panguluri, Nelson & Wyman, 2017). The Australian and USA critical infrastructure cyberattacks point to supply chain compromises (Birkett, 2017; Chung, 2018; National Institute of Standards and Technology (NIST), 2018; Srinivas, Das & Kumar, 2019). Some of the challenges of implementing cybersecurity safeguards on critical infrastructure, including 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.	Rasekh et al. (2016), CISA (2020), Bernieri and Pascucci (2019)
Increased cyber connectivity	Introduction of internet communication protocols to ICSs exposes them to security risks through the IT domain.	Hassanzadeh et al. (2020), Krotofil, Kursawe and Gollmann (2019), Rasekh et al. (2016)
False sense of security by obscurity	Older supervisory control and data acquisition systems were isolated from corporate IT networks. With increasing cyber connectivity, they become difficult to secure due to design for safety and performance.	Clark, Hakim and Panguluri (2018), Krotofil et al. (2019)
Network misconfigurations	Vulnerable computer network as a result of the misconfiguration of the firewall and related tools.	Janke et al. (2014), Panguluri, Phillips and Cusimano (2011), Ranathunga, Roughan, Nguyen, Kernick and Falkner (2016)
No media protection enforcement	Data theft due to a lack of removable media policy enforcement.	Pretorius and Van Niekerk (2016)
Unsecured remote access	Remote access to ICSs through untrusted devices, usually by third-party contractors and vendors increases cyber risk.	Krotofil et al. (2019), Stellios, Kotzanikolaou and Psarakis (2019)
Undocumented policies and procedures	Undocumented cybersecurity policies and procedures make enforcement and compliance difficult. This inevitably increases organisational cyber risk.	Clark et al. (2017), Panguluri et al. (2011)
Untrained personnel	Training and awareness of staff achieves significant cybersecurity improvements. The opposite also applies.	Clark et al. (2017), McNabb (2012), Noble, Manalo, Miller and Ferro (2017)

The above-mentioned challenges of implementing cybersecurity safeguards for water-related and other critical infrastructure are mostly at an organisational level (Gourisetti, Mylrea & Patangia, 2020). 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, track and monitor emerging cybersecurity technologies, increase cyber risk awareness and training among citizens and highlight best practices for different sectors (Brechbühl, Bruce, Dynes & Johnson, 2010).

But what are the international best practices of a good and balanced national cybersecurity policy? Recommendations have been made over the years that indicate that good national cybersecurity policies share common characteristics as summarised in Table 2 (Alexander et al., 2020; Birkett, 2017; Brechbühl, Bruce, Dynes & Johnson, 2010; Burmeister, Phahlamohlaka & Al-Saggaf, 2015; Dalton, Jansen Van Vuuren & Westcott, 2017; Detecon, 2013; Galinec, Moznik & Guberina, 2017; Greiman, 2015; NIST, 2018; Organisation for Economic Cooperation and Development (OECD), 2012; Sutherland, 2017; Timmers, 2018).

Table 2. Best-practice national cybersecurity policy characteristics

Characteristic	Key theme
The *approach* to adopt a national cybersecurity *strategy*	Cybersecurity governance
A *strategy* that is supported by *senior government officials*	Cybersecurity governance Role and responsibility
A *strategy* that is *efficiently coordinated* and *adapted* specifically to the culture and government style of a country to *holistically* address *cybersecurity requirements* of the nation	Cybersecurity governance Role and responsibility
A *strategy* that also involves *stakeholders* outside of *government*	Cybersecurity governance Stakeholders
A *strategy* that encourages flexible *policy solutions*	Cybersecurity governance Legislation and/or policies
A *strategy* that fosters *public-private partnerships* and *self-regulation* to support industry on cybersecurity	Cybersecurity governance Stakeholders Legislation and/or policies
A *strategy* that respects a nation's *foundational values* with proper *controls* and *checks and balances*	Cybersecurity governance Cybersecurity resilience Legislation and/or policies
A *strategy* that enables *collaboration* and cooperation with *international partners* in *cyberspace*	Cybersecurity governance Role and responsibility Legislation and/or policies
A *strategy* that, through appropriate *policy measures,* provides for the *generation of* accurate, valid, complete and unique *data*, to enable informed and better *policy making* as well as improved *risk assessment* outcomes	Cybersecurity governance Cybersecurity resilience Role and responsibility Legislation and/or policies
A *strategy* with all the above characteristics to achieve *nation state cyber defence capabilities* to *protect critical infrastructure, fight cybercrime* and *attain cyber resilience*, while *developing the industrial and technological resources* for cybersecurity	Cybersecurity governance Cybersecurity resilience Role and responsibility Legislation and/or policies

The characteristics of a balanced national cybersecurity policy yield five key themes from Table 2:

- Cybersecurity governance
- Cybersecurity resilience
- Stakeholders
- Role and responsibilities
- Legislation and/or policies

These five themes were utilised to conduct a detailed analysis of the South African national cybersecurity and water and sanitation legislative and policy environments as shown in Appendix A. Thematic analysis techniques were then applied and results integrated through systems thinking to make sense of the findings as discussed in the next two chapters.

The 2001 Budapest Convention on cybercrime is the only viable international cooperation instrument on fighting cybercrime. However, it will only be 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. This may prove difficult for developing nations. As a developing nation, South Africa's domestic legislation and international cooperation mechanisms are reviewed in the next chapter, with a particular focus on water and sanitation.

3. NATIONAL CYBERSECURITY POLICY ENVIRONMENT AND PRACTICES

3.1 Introduction

To develop an effective cybersecurity strategy for the water and wastewater sector, it is prudent to first understand policy discussions at national level (Alexander et al., 2020). On 23 March 2012, the National Cybersecurity Policy Framework (NCPF) was adopted by the South African Cabinet (Jansen van Vuuren et al., 2014; Kshetri, 2015; Ntsaluba, 2017; Wolfpack, 2012) and gazetted by the Minister of State Security on 23 September 2015 (South Africa, 2015). 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" (South Africa, 2015:15). The NCPF's supporting legislation and policies were reviewed to determine where and how the water and wastewater sector fits in, if at all.

The NCPF has since been reviewed 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 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.

3.2 National cybersecurity stakeholders

Review work of the national cybersecurity stakeholders was conducted (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 in 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 2. The key organs of state that play a critical role in the implementation of the cybersecurity strategy (South Africa, 2015) are dominated by the Justice, Crime Prevention and Security (JCPS) cluster (Mutemwa, Mtsweni & Mkhonto, 2017). According to the government of South Africa (2020), 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. The South African national cybersecurity governance structure is shown in Figure 2.

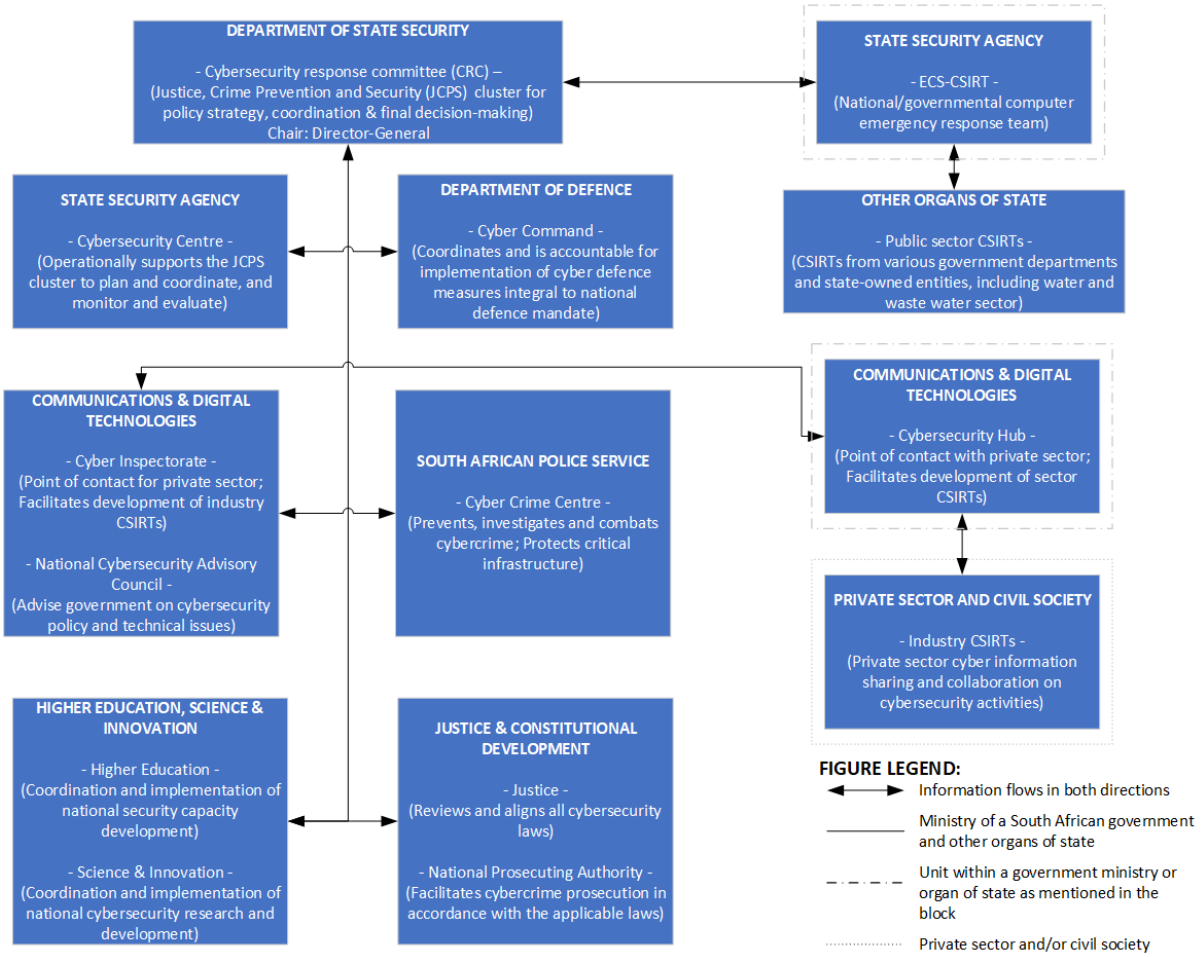

Figure 2. National cybersecurity governance structure in South Africa

In Figure 2, the bidirectional arrows are not reporting lines. They represent information flow within and outside the national cybersecurity system. All other organs of state, including but not limited to those listed above, are required to align their cybersecurity and ICT policies and practices with the NCPF (South Africa, 2015). In effect, Figure 2 shows the cybersecurity coordination and management structure in South Africa. The coordination is performed by the JCPS Cybersecurity Response Committee (CRC) (Government SA, 2020), which is operationally supported by the Cybersecurity Centre in the SSA (South Africa, 2015). This interministerial coordination is managed and facilitated through various pieces of legislation and government policies.

3.3 National cybersecurity legislation and policies

Review work of legislation and government policies used for the implementation of the national cybersecurity strategy was conducted (Appendix A). Similarly, legislation and policies that are mentioned multiple times in Appendix A are listed once below.

All other 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 (South Africa, 2015), the Electronic Communications Security (Pty) 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 (Detecon, 2013; Sutherland, 2017). This is the legal framework for national cybersecurity governance and resilience in South Africa. Harmonising and aligning these (Detecon, 2013) could make the currently complex coordination and management of the national cybersecurity endeavours (Sutherland, 2017) a bit easier. In addition to the Constitution (South Africa, 1996), 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 mentioned repeatedly. These are shown in Figure 3 (South Africa, 2000, 2002, 2003, 2013, 2015, 2019, 2020).

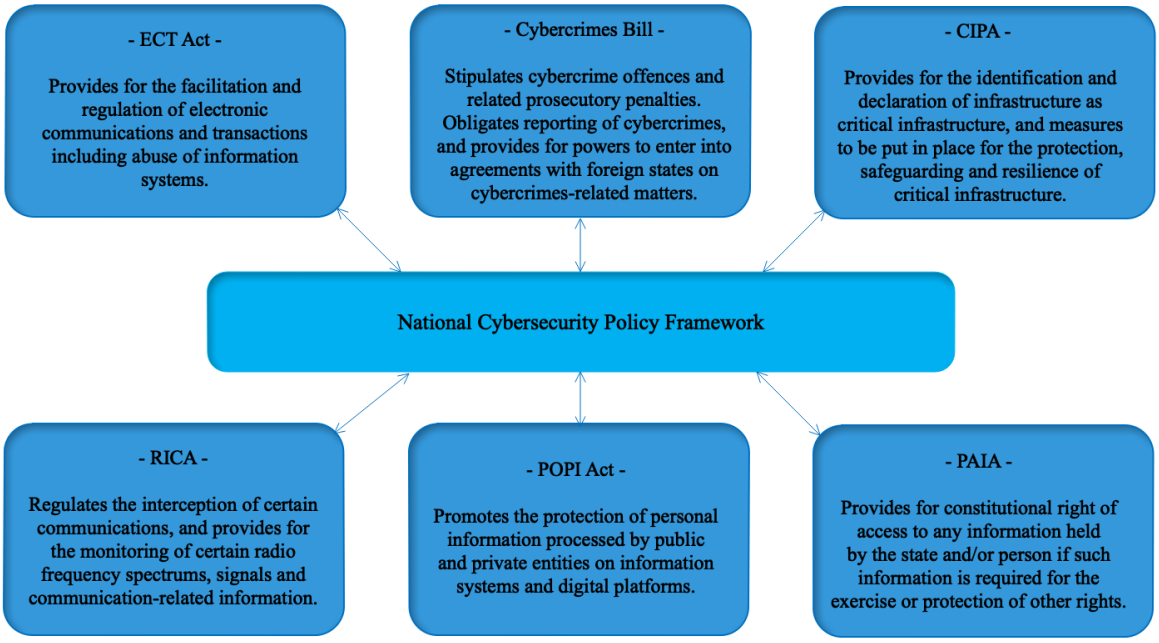

Figure 3. Key national cybersecurity policy and legislation in South Africa

Review of the six individual pieces of legislation and one policy in Figure 3 reveals 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 3 as they relate to cybersecurity and cybercrimes in South Africa.

Table 3. 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.

There are many other repeals and amendments but those are beyond the scope of the study. However, it is imperative to highlight that, as shown in Table 3, sections 85 to 88 (cybercrime offences) of the ECT Act (South Africa, 2002), being one of the key cybersecurity laws in South Africa, have since been repealed and replaced by sections 2 to 12 of the newly approved Cybercrimes Bill (South Africa, 2020). 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 reveals a few implementation deficits and challenges.

3.4 National cybersecurity challenges

Apart from the fact that the current coordination and management of the national cybersecurity strategy of South Africa is complex and should be simplified (Detecon, 2013; Sutherland, 2017), the review work (Appendix A) reveals a few implementation deficits. Although more than ten implementation deficits are revealed, these can be aggregated into the ten described in Table 4.

Table 4. National cybersecurity policy implementation deficits

Deficit	Description
Poor public-private partnerships track record	There is generally a poor track record of interministerial 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 refer 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 cyberthreats 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

Deficit	Description
	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 protect the national critical infrastructure effectively 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.
Lack of commitment to existing security conventions	There are no visible commitments to existing conventions such as the Budapest Convention and AU 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 interministerial 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.

Some of the challenges in Table 4 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 (Karabacak, Yildirim & Baykal, 2016). Identifying and classifying critical infrastructure and updating the inventory on a regular basis is a challenge (Tiirmaa-Klaar, 2016). This is highlighted by White (2019) in regard to the American Department of Homeland Security's need to develop guidelines to classify critical infrastructure sectors. In the case of Turkey (Karabacak et al., 2016), what was found was that if a sector is predominantly managed by private entities, the general cybersecurity risk levels tend 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 (De Bruijn & Janssen, 2017). The complex nature of the current coordination and management of the national cybersecurity strategy (Detecon, 2013; Sutherland, 2017) may not be unique to South Africa after all.

Key national cybersecurity stakeholders, including governance structure, legislation and policies, were discussed in this chapter. Additionally, the national cybersecurity policy implementation deficits were highlighted. It is important to understand how these national cybersecurity policy implementation deficits impact the water and wastewater sector's cybersecurity responsibilities. In this regard, the next chapter is a review of whether and how the water and wastewater legal context addresses protection of the sector's cyber critical infrastructure.

4. WATER SECTOR POLICY ENVIRONMENT AND PRACTICES

4.1 Introduction

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) (South Africa, 1996). These constitutional rights mandate the state in section 27(2) of the Constitution, through the Department of Water and Sanitation (DWS), to ensure that the water resources of the country are sustainably consumed and managed as well as protected (DWS, 2020).

4.2 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 (Government SA, 2019) and the latest DWS annual report (DWS, 2020). 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 (DWS, 2020; Government SA, 2019):

- 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 legal framework is required for ensuring that the water resources of the country are sustainably consumed, managed and protected.

4.3 Water legislation and policies

Sources from Government SA (2020b), Makaya et al. (2020), Socio-economic Rights Institute (SERI) (2020) and Stuart-Hill and Schulze (2010) were reviewed to identify legislation and policies governing the water and wastewater sector of South Africa. Similar legislation and government policies in the sources are listed once below. All other 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 legislation and policies above. The idea was to determine if and whether provisions for cyber protection of critical infrastructure are made. The review reveals water cybersecurity gaps and challenges as discussed in the next section.

4.4 Deficits in the protection of water cyber critical infrastructure

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 (Pedrosa, 2020) – a technique for planning, monitoring and managing water resources in a coordinated manner. The legislation and policies contain nothing relating to the protection of cyber and physical critical infrastructure as described in Table 5.

Table 5. Deficits in protection of water cyber critical infrastructure

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 5 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 (Government SA, 2019). 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 cyber and physical critical infrastructure protection is made in any of the water and wastewater legislation and policies. A review of the existing international, national and sector (water and wastewater) cybersecurity legislative and policy environments was conducted in this section. The review identified the cybersecurity gaps and challenges in the national and water and wastewater sector. What is not clear thus far is how the water and wastewater sector interrelates with the national cybersecurity legislative and policy environment.

So far, three interdependent cybersecurity systems (international cybersecurity environment and practices; national cybersecurity environment and practices; and water sector policy environment and practices), each with its own unique purpose, have been discussed. While the international and national systems have clear cybersecurity-related policies and/or legislation, it would appear that 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 and national cybersecurity legislative and policy environment were examined. The results are discussed in the next chapter.

5. ANALYSIS OF INTERRELATIONS ON INTERNATIONAL, NATIONAL AND SECTOR LEVEL

5.1 Introduction

The interdependent cybersecurity relationships between three dynamic systems (international, national and water sector systems) as well as how they can interoperate effectively are illustrated in Figure 4.

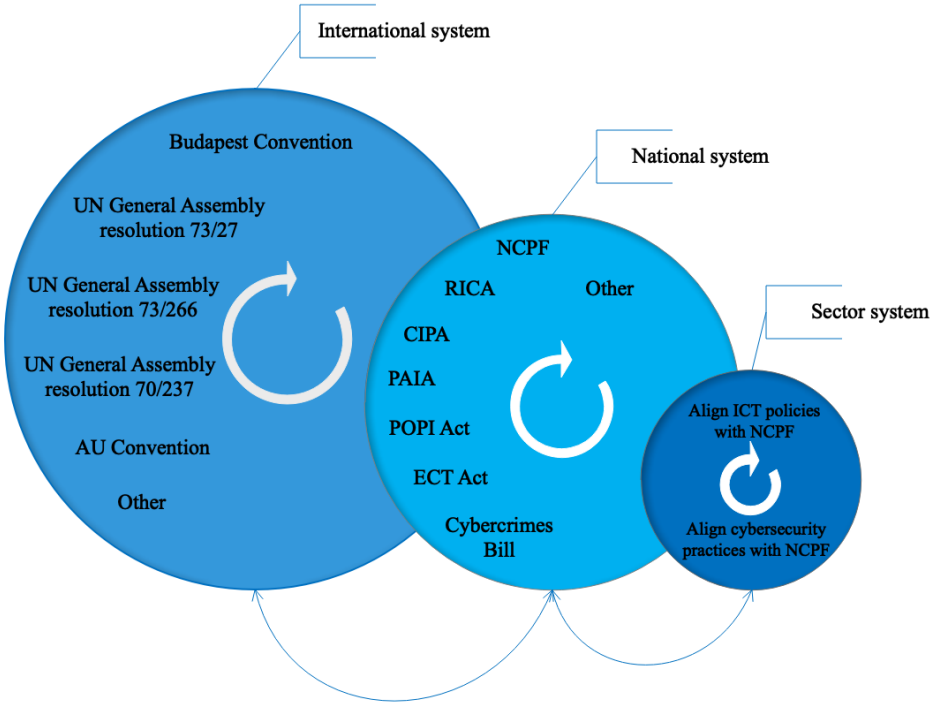

Figure 4. Dynamic interrelationships of cybersecurity systems

Adapted from Brechbühl et al. (2010)

The arrows in Figure 4 represent cybersecurity information flow within and between the three interdependent systems. Clough (2014) indicates that nation states should put in place domestic legislation that is conducive for international cooperation such as the Budapest Convention. Coleman (2019) 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.

The interrelationships between the national cybersecurity legislative and policy environment (national system in Figure 4) and water and wastewater sector legislative and policy

environment (sector system in Figure 4) were also analysed. This was aimed at contextualising the water and wastewater sector's cybersecurity responsibilities within the national cybersecurity legislative and policy environment.

5.2 Research approach

The systems thinking approach (Meadows, 2008; Senge, 2006) is employed. 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 (Meadows, 2008; Senge, 2006). It is an analysis tool to identify and understand how the parts interconnect within the entire system (Ramos, 2013). This is especially useful when considering the complex nature of government policy and the different parties involved in effecting legislation. 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 (Schuster, 2018). Secondly, the elements of a system are the most visible and are the actors in the system. It is however acknowledged that some elements can be more important than others (Meadows, 2008). Changing system elements has the least impact on a system (Meadows, 2008), provided that the function of the system remain unaltered (Schuster, 2018). Thirdly, interconnections are oftentimes harder to see but more critical in the system than elements (Meadows, 2008; Schuster, 2018). They are the signals that enable one element of a system to respond to other elements through action or decision points (Meadows, 2008). Oftentimes, interconnections are not physical flows (Meadows, 2008; Schuster, 2018), but rather the flow of influences, energy, or information inside and outside the system as it strives towards a state of equilibrium (Chowdhury, 2019; Fiksel, 2015).

To closely examine the interrelationships between the water and wastewater sector and national cybersecurity legislative and policy environment, the four steps are sequentially operationalised were:

Step 1: Identify the National Cybersecurity System Function, Actors and Interconnections

Step 2: Identify the Water and Wastewater System Function, Actors and Interconnections

Step 3: Identify the Water and Wastewater System as An Actor in the National Cybersecurity System

Step 4: Analyse Interrelations between the Water and Wastewater and National Cybersecurity Systems

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. The findings are summarised in Table 6.

Table 6. Summary of 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

In Table 6, 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 6 are discussed in the next four sections.

5.3 Results

Four systems thinking steps were executed in the literature review in Appendix A and discussed in Chapters 3 and 4. These systems thinking analysis results are detailed in sections 5.2.1 to 5.2.4.

5.2.1 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 implementing the six key objectives of the national cybersecurity (function), as well as to identify legislation and policies (interconnections) governing the interrelationships between stakeholders. The function of the national cybersecurity strategy has already been defined in section 3.1 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” (South Africa, 2015:15). 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 between the stakeholders in the national cybersecurity system. These are the interconnections of the national cybersecurity legislative and policy environment. As argued by Sutherland (2017) and Detecon (2013), 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 and appoint cyber inspectors. Firstly, no Cyber Inspectorate has ever been established and cyber inspectors have yet to be appointed. 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 cybercrime in South Africa.

5.2.2 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 protection of the cyber water-related infrastructure (function), identify the legislation and policies (interconnections) responsible for the functions and determine whether these delineate cybersecurity-related roles and responsibilities. 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 4.2.

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 4.3. These determine the interrelationships between 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 (2016) refers to as an independent system (see sector system in Figure 4) consisting of its own components configured in such a way as to achieve its unique purpose within the national system.

5.2.3 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 represent the water and wastewater sector as an actor or stakeholder within the bigger national cybersecurity system.

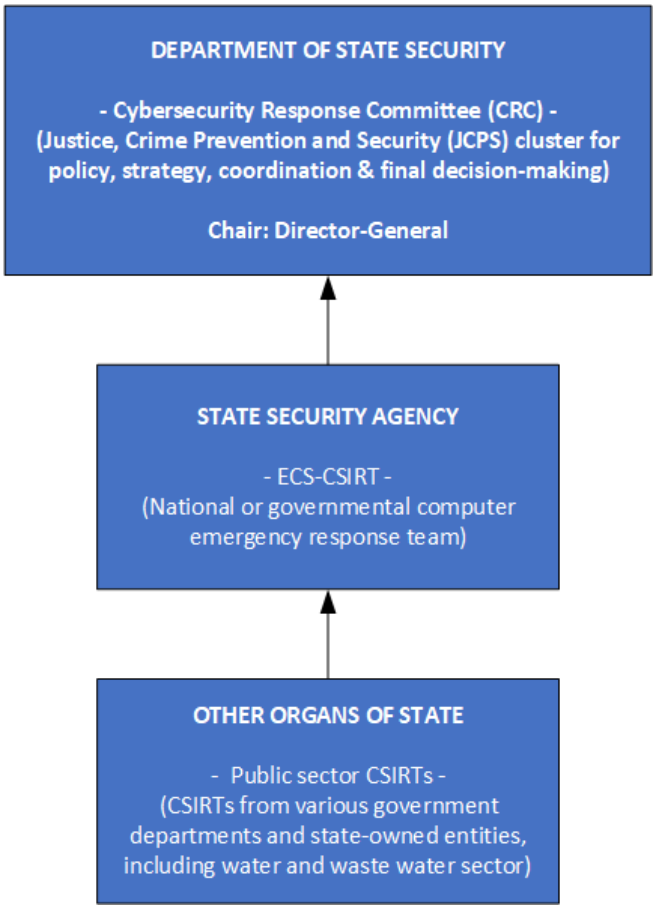

Figure 5. Water and wastewater system as an actor within the national cybersecurity system

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 (2017), 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.

5.2.4 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 roles and responsibilities. It was found that the water and wastewater legislation and policies make no provision for the protection of the sector's cyber and physical critical infrastructure. Instead, analysis revealed that the cybersecurity roles and responsibilities to protect the sector's cyber and physical critical infrastructure, and indeed that of other sectors, are drawn mainly from the NCPF (South Africa, 2015), Cybercrimes Bill (South Africa, 2020), CIPA (South Africa, 2019), POPI Act (South Africa, 2013), RICA (South Africa, 2003), ECT Act (South Africa, 2002) and PAIA (South Africa, 2000). For example, the NCPF states that the SSA is, among other things, required to "initiate and lead a process" (South Africa, 2015:27) 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 (South Africa, 2015:18).

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 other things, 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" (South Africa, 2015:18-19). 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.

Systems thinking analysis results presented in this chapter have shown that 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 discussed in detail in the next chapter.

6. DISCUSSIONS

6.1 Introduction

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 interrelations. 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.

6.2 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 (2008), 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 indicate 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 (Meadows, 2008), systems thinking indicates that changing individual stakeholders should have the least impact on the national cybersecurity programme, provided that the purpose, 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 indicate 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 (as of 10 November 2020) yet to ratify the Budapest Convention of 2001 (Budapest Convention, 2020). 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 piece of 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 a 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 between 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 (Sutherland, 2020) is not encouraging. It was also found that the no less than 37 different pieces of legislation and policies lead 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 and appoint cyber inspectors, it has failed to report any activities by the National Cybersecurity Advisory Council, if any, and progress to ensure the establishment of industry and sector CSIRTs as stipulated in the NCPF since it was gazetted in 2015 is slow. 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 conspicuously absent in the coordination of these activities. As already alluded to by Detecon (2013) and corroborated by Gcaza (2018), 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 (Mahlaka, 2020) 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 achieve 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 (Merten, 2020). 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 et al. (2017), 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 (Timmers, 2018). 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 cybercrime 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 (Burmeister et al., 2015), and thus retroactive, than offensive which requires proactiveness (Flowers & Zeadally, 2014). It is more passive and static than proactive. Under international laws, any sovereign state has the right to defend itself against adversarial actors (Flowers & Zeadally, 2014). 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" (South Africa, 2015:24). Defence (retroactive approach) seems to be South Africa's 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.

6.3 Water and wastewater legislative and policy environment

The study findings indicate that two functions of the water and wastewater sector are 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 consisting 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 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 (South Africa, 2015).

The findings also indicate 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 (South Africa, 2015:18-19) 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 point (2017), 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.

This chapter dealt with how stakeholders in both the national cybersecurity and water and wastewater systems interrelate through legislation and policies to achieve the national cybersecurity function or purpose. By understanding the dynamic nature of the interconnected relationships (Van Woensel, 2020; Fiksel, 2015; Senge, 2006) between various stakeholders, it is concluded that the water and wastewater sector is immediately able to develop its own cybersecurity governance framework and resilience strategy as illustrated in Figure 6.

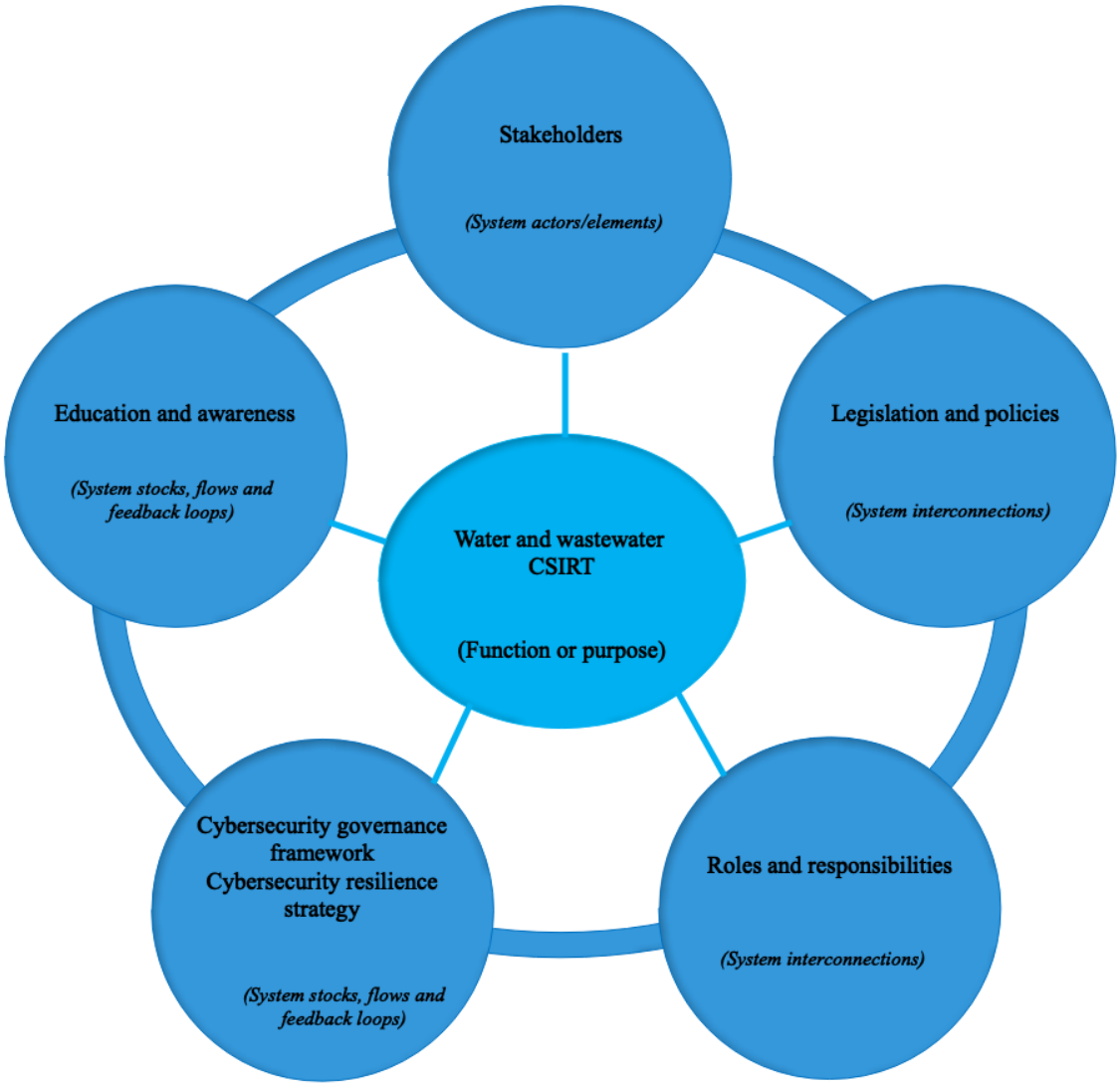

Figure 6. Water and wastewater cybersecurity system

De Jong, Neulen and Jansma (2019) 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 (De Jong et al., 2019; Karlsson, Holgersson, Söderström & Hedström, 2012). 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 chapter.

7. 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. Implementation of all the national cybersecurity legislation and policy environment recommendations are beyond the scope of the current project. The recommendations are as follows:

- The National Cybersecurity Advisory Council, and/or Cybersecurity Hub and/or Cyber Inspectorate should either be moved from the DCDT, or their operating models and mandates should 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 cybercrime in the short term, South African law enforcement agencies may need to partner with international stakeholders such as Interpol and similar others to develop cybercrime 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 cybercrime 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 to existing ones, it is recommended that a sector-specific agency be established. This would indeed require either the development of a new piece of legislation or amendment to 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. The implementation of this recommendation is beyond the scope of the current project.
- *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. This recommendation will be achieved as part of the WP2 deliverable in the current project.

- *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 facilitate the exchange of cybersecurity information, sharing of knowledge and collaboration, skills development and rapid responses to incidents. This recommendation will be achieved as part of the WP3 deliverable in the current project.
- *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. This recommendation will be achieved as part of the WP3 and WP4 deliverables in the current project.
- *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. This recommendation will be achieved as part of the WP4 deliverable in the current project.

- *Develop a sector cybersecurity awareness campaign strategy*. Coordinated sector-wide cybersecurity education and awareness campaigns should become regular occurrences. This recommendation will be achieved as part of the WP4 deliverable in the current project.

8. CONCLUSIONS: WATER AND SANITATION CYBERSECURITY LEGISLATIVE AND POLICY ENVIRONMENT

The national cybersecurity strategy is a system comprising mainly 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 between 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 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. However, 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 examine 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.

REFERENCES

Alexander, A., Graham, P., Jackson, E., Johnson, B., Williams, T., & Park, J. (2020). An analysis of cybersecurity legislation and policy creation on the state level. In K. Choo, T. Morris, & G. Peterson (Eds.), *National Cyber Summit (NCS) Research Track. NCS 2019. Advances in Intelligent Systems and Computing* (Vol. 1055, pp. 30-43). https://doi.org/10.1007/978-3-030-31239-8_3.

AU Convention. (2020). List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection. Retrieved 5 November 2020, from https://au.int/sites/default/files/treaties/29560-sl-AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.pdf.

Bernieri, G., & Pascucci, F. (2019). Improving security in industrial Internet of Things: A distributed intrusion detection methodology. In C. Alcaraz (Ed.), *Security and privacy trends in the Industrial Internet of Things: Advanced sciences and technologies for security applications* (pp. 161-179). Cham, Switzerland.

Birkett, D., & Mala-Jetmarova, H. (2014). Plan, prepare and safeguard: Water critical infrastructure protection in Australia. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure* (pp. 287-313). https://doi.org/10.1007/978-3-319-01092-2_14.

Birkett, D. M. (2017). Water critical infrastructure security and its dependencies. *Journal of Terrorism Research*, *8*(2), 1-21.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77-101.

Brechbühl, H., Bruce, R., Dynes, S., & Johnson, M. E. E. (2010). Protecting critical information infrastructure: Developing cybersecurity policy. *Information Technology for Development*, *16*(1), 83-91. https://doi.org/10.1002/itdj.20096.

Budapest Convention. (2001). Convention on Cybercrime, European Treaty Series – No. 185. Retrieved 4 November 2020, from https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

Budapest Convention. (2020). Chart of signatures and ratifications of Treaty 185: Convention on cybercrime, status as of 05/11/2020. Retrieved 5 November 2020, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=9UQ3WQaH.

Burmeister, O., Phahlamohlaka, J., & Al-Saggaf, Y. (2015). Good governance and virtue in South Africa's cyber security policy implementation. *International Journal of Cyber Warfare and Terrorism*, *5*(1), 19-29.

Chowdhury, R. (2019). Systems thinking for management consultants: Flexible systems management. https://doi.org/10.1007/978-981-13-8530-8_1.

Chung, J. J. (2018). Critical infrastructure, cybersecurity, and market failure. *Oregon Law Review*, *96*(2), 441-476.

CISA. (2020). Alert (AA20-352A): Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations. Retrieved 18 December 2020, from https://web.archive.org/web/20201218004033/https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

Clark, R. M., & Hakim, S. (2014). Securing water and wastewater systems: Global experiences. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure*. https://doi.org/10.1007/978-3-319-01092-2.

Clark, R. M., Hakim, S., & Panguluri, S. (2018). Protecting water and wastewater utilities from cyber-physical threats. *Water and Environment Journal*, *32*(3), 384-391. https://doi.org/10.1111/wej.12340.

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Protecting drinking water utilities from cyberthreats. *Journal – American Water Works Association*, *109*(2), 50-58. https://doi.org/doi:10.5942/jawwa.2017.109.0021.

Clough, J. (2014). A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation. *Monash University Law Review*, *40*(3), 698-736.

Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race and Law*, *24*(2), 417-439.

Dalton, W., Jansen van Vuuren, J., & Westcott, J. (2017). Building cybersecurity resilience in Africa. In A. R. Bryant, J. R. Lopez, & R. F. Mills (Eds.), *Proceedings of the 12th International Conference on Cyber Warfare and Security* (Vol. 2000, pp. 112-120). Dayton, OH: Academic Conferences and Publishing International.

De Barros, M. J. Z., Lazarek, H., & Jennifer, M. (2018). Comparative study of cybersecurity policy among South Africa and Mozambique. In L. Leenen (Ed.), *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018* (pp. 521-529). Reading, United Kingdom: Academic Conferences and Publishing International.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. https://doi.org/http://dx.doi.org/10.1016/j.giq.2017.02.007.

De Jong, M. D. T., Neulen, S., & Jansma, S. R. (2019). Citizens' intentions to participate in governmental co-creation initiatives: Comparing three co-creation configurations. *Government Information Quarterly*, *36*(3), 490-500.

Detecon. (2013). E-commerce, cybercrime and cybersecurity – status, gaps and the road ahead. Retrieved 19 June 2020, from https://www.dtps.gov.za/index.php?option=com_phocadownload&view=category&download=121:20131126_policy-review_e-commerce-cybercrime-and-cybersecurity_final&id=39:e-commerce-cyber-security&Itemid=143.

Dlamini, I. Z., Taute, B., & Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. *Proceedings of Southern African Cyber Security Awareness Workshop*, 15-31. Retrieved 19 June 2020, from http://researchspace.csir.co.za/dspace/bitstream/handle/10204/5163/Dlamini_2011.pdf?sequence=1&isAllowed=y.

Dlamini, Z., & Modise, M. (2013). Cyber security awareness initiatives in South Africa: A synergy approach. In M. Warren (Ed.), *Case studies in information warfare and security* (pp. 1-22). Retrieved 19 June, from http://researchspace.csir.co.za/dspace/bitstream/handle/10204/5941/Dlamini_2012.pdf?sequence=1.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2018). *Enterprise cybersecurity study guide: How to build a successful cyberdefense program against advanced threats*. New York, NY: Apress.

DWS. (2020). Department of Water and Sanitation 2018/19 annual report, Vote 36: Water is life – sanitation is dignity. Retrieved 25 September 2020, from http://www.dwa.gov.za/documents/AnnualReports/19213_Annual_Report_201819inhouse.pdf.

Fiksel, J. (2015). Systems thinking. In J. Fiksel (Ed.), *Resilient by design: Creating businesses that adapt and flourish in a changing world* (pp. 35-50). https://doi.org/10.5822/978-1-61091-588-5_3.

Flowers, A., & Zeadally, S. (2014). US policy on active cyber defense. *Journal of Homeland Security and Emergency Management*, *11*(2), 289-308. https://doi.org/10.1515/jhsem-2014-0021.

Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. *Journal for Control, Measurement, Electronics, Computing and Communications*, *58*(3), 273-286. https://doi.org/10.1080/00051144.2017.1407022.

Gcaza, N. (2018). Cybersecurity awareness and education: A necessary parameter for smart communities. In N. Clarke & S. Furnell (Eds.), *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security and Assurance* (pp. 80-90). Dundee, Scotland: University of Plymouth Press.

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, *105*, 410-431. https://doi.org/10.1016/j.future.2019.12.018.

Government of South Africa. (2020). What are the government clusters and which are they? Retrieved 22 July 2020, from https://www.gov.za/faq/guide-government/what-are-government-clusters-and-which-are-they.

Government SA. (2019). National water and sanitation master plan, Volume 1: Call to action, version 10.1: Ready for the future and ahead of the curve. Retrieved 25 September 2020, from https://www.gov.za/sites/default/files/gcis_document/201911/national-water-and-sanitation-master-plandf.pdf.

Government SA. (2020). Water and sanitation. Retrieved 22 July 2020, from https://www.gov.za/about-sa/water-affairs.

Greiman, V. A. (2015). Cybersecurity and global governance. *Journal of Information Warfare*, *14*(4), 1-14, II.

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 03120003. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686.

Hitchins, D. (2009). What are the general principles applicable to systems? *INCOSE Insight*, *12*(4), 59-63.

Janke, R., Tryby, M., & Clark, R. M. (2014). Protecting water supply critical infrastructure: An overview. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure* (pp. 29-85). Cham, Switzerland: Springer International.

Jansen van Vuuren, J. C., Leenen, L., Phahlamohlaka, J., Zaaiman, J., Van Vuuren, J. J., Leenen, L., … Zaaiman, J. (2014). An approach to governance of cybersecurity in South Africa. *International Journal of Cyber Warfare and Terrorism*, *2*(4), 13-27. https://doi.org/10.4018/ijcwt.2012100102.

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer Law & Security Review*, *32*, 526-539.

Karlsson, F., Holgersson, J., Söderström, E., & Hedström, K. (2012). Exploring user participation approaches in public e-service development. *Government Information Quarterly*, *29*(2), 158-168. https://doi.org/https://doi.org/10.1016/j.giq.2011.07.009.

Krotofil, M., Kursawe, K., & Gollmann, D. (2019). Securing industrial control systems. In C. Alcaraz (Ed.), *Security and privacy trends in the Industrial Internet of Things: Advanced sciences and technologies for security applications* (pp. 3-26). https://doi.org/10.1007/978-3-030-12330-7_1.

Kshetri, N. (2015). Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, *18*(4), 245-249. https://doi.org/10.1080/1097198X.2015.1108093.

Mahlaka, R. (2020). Experian offers mea culpa after massive data breach blunder. Retrieved 26 August 2020, from https://www.dailymaverick.co.za/article/2020-08-23-experian-offers-mea-culpa-after-massive-data-breach-blunder/.

Makaya, E., Rohse, M., Day, R., Vogel, C., Mehta, L., McEwen, L., … Van Loon, A. F. (2020). Water governance challenges in rural South Africa: Exploring institutional coordination in drought management. *Water Policy*, *22*(4), 519-540. https://doi.org/10.2166/wp.2020.234.

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, *27*(2), 233-272. https://doi.org/10.1108/ICS-03-2018-0031.

McNabb, J. K. (2012). Securing public drinking water utilities. *Journal of the New England Water Works Association*, *127*(1), 37-59.

Meadows, D. (2008). *Thinking in systems: A primer* (D. Wright, Ed.). London, England: Earthscan.

Merten, M. (2020). SAPS regulations: It's crucial to watch critical infrastructure rules to prevent a power grab. Retrieved 3 April 2020, from https://www.dailymaverick.co.za/article/2020-04-03-saps-regulations-its-crucial-to-watch-critical-infrastructure-rules-to-prevent-a-power-grab/.

Mertens, D. (2018). *Mixed methods design in evaluation*. Thousand Oaks, CA: Sage.

Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415-428. https://doi.org/10.1108/DPRG-05-2017-0025.

Mutemwa, M., Mtsweni, J., & Mkhonto, N. (2017). Developing a cyber threat intelligence sharing platform for South African organisations. *2017 Conference on Information Communication Technology and Society*. https://doi.org/10.1109/ICTAS.2017.7920657.

NIST. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. Retrieved 19 July 2010, from https://web.archive.org/web/20201122005055/; https://www.nist.gov/cyberframework.

Noble, T., Manalo, C., Miller, K., & Ferro, C. (2017). Cybersecurity assessments of 30 drinking water utilities. *Journal of the New England Water Works Association*, *131*(4), 219-227.

Ntsaluba, N. (2017). *Cybersecurity policy and legislation in South Africa* (University of Pretoria). Retrieved 20 June 2020, from https://repository.up.ac.za/handle/2263/65706.

OECD. (2012). Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy. Retrieved 25 June 2020, from https://www.oecd.org/sti/ieconomy/cybersecurity policy making.pdf.

Panguluri, S., Phillips, W., & Cusimano, J. (2011). Protecting water and wastewater infrastructure from cyber attacks. *Frontiers of Earth Science*, *5*(4), 406-413. https://doi.org/10.1007/s11707-011-0199-5.

Pedrosa, V. A. (2020). The necessity of IWRM: The case of San Francisco river water conflicts. In E. O. Vieira, S. Sandoval-Solis, V. A. Pedrosa, & J. P. Ortiz-Partida (Eds.), *Integrated water resource management* (pp. 27-34). https://doi.org/10.1007/978-3-030-16565-9_3.

Phahlamohlaka, J., & Hefer, J. (2019). The impact of cybercrimes and Cybersecurity Bill on South African national cybersecurity: An institutional theory analytic perspective. *THREAT2019 Cybersecurity Summit*, 1-7. Retrieved from https://researchspace.csir.co.za/dspace/bitstream/handle/10204/11438/RS_The%20Impact%20of%20Cybercrimes%20and%20Cybersecurity%20Bill%20on%20South%20African_2019.pdf?sequence=1&isAllowed=y.

Pretorius, B., & Van Niekerk, B. (2016). Cyber-security for ICS/SCADA: A South African perspective. *International Journal of Cyber Warfare and Terrorism*, *6*(3), 1-16. https://doi.org/10.4018/ijcwt.2016070101.

Ramos, H. (2013). Creativity and systems thinking. In E. G. Carayannis (Ed.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 12-58). https://doi.org/10.1007/978-1-4614-3858-8_53.

Ranathunga, D., Roughan, M., Nguyen, H., Kernick, P., & Falkner, N. (2016). Case studies of SCADA firewall configurations and the implications for best practices. *IEEE Transactions on Network and Service Management*, *13*(4), 871-884. https://doi.org/10.1109/TNSM.2016.2597245.

Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., Katherine Banks, M., & Banks, M. K. (2016). Smart water networks and cyber security. *Journal of Water Resources Planning and Management*, *142*(7), 1-3. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646.

Rebovich, G., & White, B. E. (2011). *Enterprise systems engineering: Advances in the theory and practice*. Boca Raton: CRC Press.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: Global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67-81.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students.* Harlow, England: Pearson.

Schuster, S. (2018). *The art of thinking in systems: Improve your logic, think more critically, and use proven systems to solve your problems*. Scotts Valley, CA: CreateSpace Independent Publishing Platform.

SEBoK Editorial Board. (2020). The g*uide to the systems engineering body of knowledge (SEBoK), v. 2.3*. Hoboken, NJ: BKCASE.

Senge, P. M. (2006). *The fifth discipline: The art and practice of the learning organization*. New York, NY: Doubleday, Random House.

SERI. (2020). Water and sanitation legislation and regulations. Retrieved 22 August 2020, from https://www.seri-sa.org/index.php/links/policy-and-legislation/15-links/policy-and-legislation/87-water-and-sanitation.

South Africa. (1996). South African Constitution. Retrieved 17 September 2020, from https://www.justice.gov.za/legislation/constitution/SAConstitution-web-eng.pdf.

South Africa. (2000). Promotion of Access to Information Act 2 of 2000. Retrieved 19 July 2020, from https://www.justice.gov.za/legislation/acts/2000-002.pdf.

South Africa. (2002). Electronic Communications and Transactions Act 25 of 2002. Retrieved 19 June 2020, from https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.

South Africa. (2003). https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13. Retrieved 17 July 2020, from https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf.

South Africa. (2013). Protection of Personal Information Act 4 of 2013. Retrieved 18 July 2020, from https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

South Africa. (2015). National Cybersecurity Policy Framework (NCPF). Retrieved 10 April 2020, from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf.

South Africa. (2019). Critical Infrastructure Protection Act 8 of 2019. Retrieved 15 June 2020, from https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf.

South Africa. (2020). Cybercrimes Bill (B6-2017). Retrieved 29 July 2020, from https://pmg.org.za/bill/684/?via=homepage-card.

Spathoulas, G., & Katsikas, S. (2019). Towards a secure Industrial Internet of Things. In C. Alcaraz (Ed.), *Security and privacy trends in the Industrial Internet of Things: Advanced sciences and technologies for security applications* (pp. 29-45). https://doi.org/10.1007/978-3-030-12330-7_2.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178-188.

Stellios, I., Kotzanikolaou, P., & Psarakis, M. (2019). Advanced persistent threats and zero-day exploits in Industrial Internet of Things. In C. Alcaraz (Ed.), *Security and privacy trends in the Industrial Internet of Things: Advanced sciences and technologies for security applications* (pp. 47-68). https://doi.org/10.1007/978-3-030-12330-7_3.

Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world.* New York, NY: Irwin/McGraw-Hill.

Stuart-Hill, S. I., & Schulze, R. E. (2010). Does South Africa's water law and policy allow for climate change adaptation? *Climate and Development, 2*(2), 128-144. https://doi.org/10.3763/cdev.2010.0035.

Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication*, *20*, 83-112. https://doi.org/10.23962/10539/23574.

Sutherland, E. (2020). The Fourth Industrial Revolution – The case of South Africa. *Politikon*, *47*(2), 233-252. https://doi.org/10.1080/02589346.2019.1696003.

Tiirmaa-Klaar, H. (2016). Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*, *1*(1), 94-106. https://doi.org/10.1080/23738871.2016.1165716.

Timmers, P. (2018). The European Union's cybersecurity industrial policy. *Journal of Cyber Policy*, *3*(3), 363-384. https://doi.org/10.1080/23738871.2018.1562560.

UN. (2020a). Open-ended working group. Retrieved 5 November 2020, from https://www.un.org/disarmament/open-ended-working-group/.

UN. (2020b). Group of governmental experts. Retrieved 5 November 2020, from https://www.un.org/disarmament/group-of-governmental-experts/.

UN. (2015). Resolution adopted by the General Assembly on 23 December 2015. Retrieved 5 November 2020, from https://undocs.org/en/A/RES/70/237.

UNECE. (2019). Working Party on Regulatory Cooperation and Standardization Policies (WP.6) – Report on the sectoral initiative on cyber security. Retrieved 17 December 2020, from https://web.archive.org/web/20201217093616/https://undocs.org/pdf?symbol=en%2FECE%2FCTCS%2FWP.6%2F2019%2F9.

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

Van Woensel, L. (2020). Systems thinking and assessing cross-policy impacts. In L. Van Woensel (Ed.), *A bias radar for responsible policy-making: Foresight-based scientific advice.* (pp. 69-84). https://doi.org/10.1007/978-3-030-32126-0_4.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security, 26*(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025.

Weiss, J. (2014). Industrial control system (ICS) cyber security for water and wastewater systems. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure* (pp. 87-105). https://doi.org/10.1007/978-3-319-01092-2_3.

White, R. (2019). Risk analysis for critical infrastructure protection. In D. Gritzalis, M. Theocharidou, & G. Stergiopoulos (Eds.), *Critical infrastructure security and resilience. Advanced sciences and technologies for security applications* (pp. 35-54). https://doi.org/10.1007/978-3-030-00024-0_3.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*, 63-72. https://doi.org/10.1365/s43439-020-00012-5.

WMO. (2020). Water and cyber security – Protection of critical water-related infrastructure. Retrieved 17 December 2020, from https://web.archive.org/web/20201118080434/https://public.wmo.int/en/events/meetings/water-and-cyber-security-protection-of-critical-water-related-infrastructure-online.

Wolfpack. (2012). The South African cyber threat barometer: A strategic public-private partnership (PPP) initiative to combat cybercrime in SA. Retrieved 17 July 2020, from 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.

WSIS. (2020). Basic information: About WSIS. Retrieved 5 November 2020, from https://www.itu.int/net/wsis/basic/about.html.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, *39*(1), 93-112.

https://doi.org/10.1177/0739456X17723971.

APPENDIX A: National Cybersecurity Policy Framework Analysis

A literature review of the previous analysis work on the National Cybersecurity Policy Framework (NCPF) was conducted using the systems thinking method. This considered mainly the stakeholders involved (elements/actors in systems thinking), legislation and policies (interconnections in systems thinking) underpinning the national cybersecurity strategy and the implementation deficits of the NCPF. 'Stakeholders' and 'legislation and policies' are also two of the five best-practice cybersecurity policy analysis themes derived from Table 2.

Researcher	Stakeholders (Elements/Actors)	Legislation and Policies (Interconnections)	Implementation deficits
Phahlamohlaka and Hefer (2019)	*Domestic* • Cybersecurity Centre (SSA) • Cyber Crime Centre (SAPS) • Cybersecurity Hub (Department of Telecommunications and Postal Services) • Cyber Command (DoD)		
De Barros, Lazarek and Jennifer (2018)	*Foreign* • International Telecommunication Union (ITU)	• NCPF	
Dalton et al. (2017)	*Foreign* • African Union (AU)	• African Union Convention on Cybersecurity and Personal Data Protection	
Ntsaluba (2017)	*Domestic* • Justice, crime prevention and security (JCPS) cluster (SSA and others) • Cybersecurity Response Committee (CRC) • Department of Telecommunications and Postal Services (DTPS) • SITA • Department of Science and Technology • Department of International Relations and Cooperation (DIRCO) • South African Revenue Service (SARS) *Foreign* • Interpol	• Constitution of the Republic of South Africa • Computer Evidence Act 57 of 1983 • Copyright Act 98 of 1978 • Critical Infrastructure Bill of 2017 • Cybercrimes and Cybersecurity Bill of 2017 • ECT Act 25 of 2002 • Electronic Communications Act 36 of 2005 • Films and Publications Act 65 of 1996 • Financial Intelligence Centre Act (FICA) 38 of 2001 • National Prosecutions Act 32 of 1998 • Monitoring and Prohibition Act 127 of 1992 • Prevention of Organised Crime Act 38 of 1999 • Promotion of Access to Information Act (PAIA) 25 of 2002	• New laws and institutions are required in South Africa to address cybersecurity requirements effectively. • 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. • New cybersecurity capabilities have to be developed and acquired by South Africa.

Researcher	Stakeholders (Elements/Actors)	Legislation and Policies (Interconnections)	Implementation deficits
		• Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 • Protection of Personal Information (POPI) Act 4 of 2013 • RICA 70 of 2002	
Mutemwa et al. (2017)	*Domestic* • South African National Defence Force (SANDF) • JCPS cluster	• NCPF • Defence Review • Cybercrimes and Cybersecurity Bill	
Sutherland (2017)	*Domestic* • Department of State Security • SSA • SSA Cybersecurity Centre • Electronic Communications Security—Cyber Security Incidents Response Team (ECS-CSIRT) • Department of Justice and Constitutional Development • NPA • SAPS • DoD • Cyberwarfare Command • Centre Headquarters (HQ) • COMSEC Ltd • Department of Telecommunications and Postal Services • National Cybersecurity Advisory Council • National Cybersecurity Hub • Cyber Inspectorate • Department of Trade and Industry • Public Service and Administration • SITA • Foreign • Forum for Incident Response and Security Teams (FIRST)	• Section 198 of the 1996 Constitution • NCPF • RICA 70 of 2002 • Protection of State Information Bill • POPI Act 4 of 2013 • Cybercrimes and Cybersecurity Bill • Cyber Warfare Strategy • ECT Act 25 of 2002 • Cryptography Regulations • E-government strategy and roadmap • Companies Act 71 of 2008 • PAIA 2 of 2000 • Corporate Governance of ICT Framework • 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 have been promulgated to establish this unit. • 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. • The proposed coordination mechanisms in the NCPF are complex, thus making their management difficult. This is exacerbated by a poor track record of interministerial coordination of programmes. Additionally, there are only limited review and oversight mechanisms, and many activities are shrouded in secrecy. • 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.
Van Niekerk (2017)	*Domestic* • SSA	• NCPF • ECT Act 25 of 2002 • RICA 70 of 2002	

Researcher	Stakeholders (Elements/Actors)	Legislation and Policies (Interconnections)	Implementation deficits
		• POPI 4 of 2013 • Cybercrimes and Cybersecurity Bill	
Pretorius and Van Niekerk (2016)		• NCPF • National Key Points Act 102 of 1980 • ECT Act 25 of 2002 • King III Report on Corporate Governance	
Kshetri (2015)	*Domestic* • Department of Communications • National Cybersecurity Advisory Council (NCAC) *Foreign* • Council of Europe (CoE)	• NCPF • 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.
Detecon (2013)	*Domestic* • State Security Agency (SSA) • South African Policy Service (SAPS) • Department of Justice and Constitutional Development (DOJ & CD) • National Prosecuting Authority (NPA) • Department of Communications (DOC) • Department of Defence and Military Veterans (DoD & MV) • Department of Science and Technology (DST) • Foreign • African Union • Southern African Development Community (SADC) • Commonwealth	• Films and Publication Act 65 of 1996 • Protection from Harassment Act 17 of 2011 • Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) 70 of 2002 • Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 • Copyright Act 98 of 1978 • Consumer Protection Act 68 of 2008 • National Archives and Record Service of South Africa Act 43 of 1996 • Trade Marks Act 194 of 1993 • Designs Act 195 of 1993 • Electronic Communications Act 36 of 2005 • Electronic Communications and Transactions Act 25 of 2002 (ECT Act) • Independent Communications Authority of South Africa (ICASA) Act 13 of 2000 • Inter-Governmental Relations Framework of 2005 • Competition Act 89 of 1998 • Broadband Infraco Act 33 of 2007	• 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. • Advanced cybersecurity strategies include protection of critical infrastructure as a key element. The ECT Act also alludes to the protection of this infrastructure. However, the implementation of protection is still in abeyance. The country had planned for critical infrastructure protection of the following priority sectors: i) energy; ii) ICT; and iii) transport. • Sector CSIRTs have not yet been established. These would be effective for incident responses and information exchange between sectors. • 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. • 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. • 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. • 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)	Implementation deficits
		• State Information Technology Agency (SITA) Act 88 of 1998 • Public Service Act: Regulation	
Dlamini and Modise (2013)		• 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.