

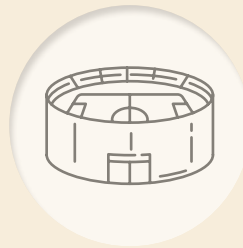
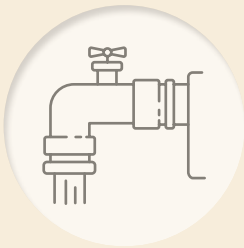
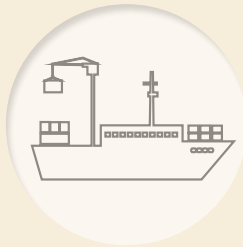


PSIRA
Private Security Industry Regulatory Authority



THE PRIVATE SECURITY
in the Protection of South African
Critical Infrastructures

SAFER HOMES
BUSINESSES
COMMUNITIES





PSiRA

Private Security Industry Regulatory Authority

Report:

**The Private Security
in the Protection of
South African Critical
Infrastructures**

ABOUT THE REPORT

Title : The Private Security in the Protection of South African Critical Infrastructures

Author : Hloniphani Xulu

Publisher : Private Security Industry Regulatory Authority©

Year Published : 2024

Special Thanks : To all those who reserved their precious time to participate in this study and the entire Research and Development team for their meaningful contribution.

TABLE OF CONTENTS

- ABOUT THE REPORT 4**
- ABBREVIATIONS AND ACRONYMS 6**
- EXECUTIVE SUMMARY 7**
- 1. INTRODUCTION 9**
- 2. BACKGROUND OF THE STUDY 11**
- 3. RESEARCH AIM, HYPOTHESIS, OBJECTIVES AND QUESTIONS..... 13**
- 4. RESEARCH METHODOLOGY 14**
- 5. LITERATURE REVIEW 16**
 - 5.1 History of critical infrastructure protection and the involvement of the private security industry..... 16
 - 5.2 The protection of critical infrastructures against cyber-threats 17
 - 5.3 The conduct of security service providers 19
 - 5.4 The formation of critical infrastructure protection regulator 19
- 6. RESEARCH FINDINGS 21**
 - 6.1 The key areas of critical infrastructure protection 21
 - 6.2 The regulatory mechanisms in the protection of critical infrastructures.... 23
 - 6.3 The level of adequacy of security training 31
 - 6.4 The conduct of security service providers in critical infrastructures..... 35
- 7. RECOMMENDATIONS..... 40**
 - 7.1 Regulation of cybersecurity personnel and companies 40
 - 7.2 Registration of critical infrastructure protection 40
 - 7.3 Establishment of database for critical infrastructures..... 41
 - 7.4 Development of regulations for critical infrastructures 41
 - 7.5 Inspections of critical infrastructure security services 42
 - 7.6 The establishment of a committee 42
 - 7.7 Development of training for critical infrastructure protection 43
- 8. CONCLUSION 44**
- REFERENCES 45**

ABBREVIATIONS AND ACRONYMS

ABET	Adult Basic Education and Training
CCMA	Commission for Conciliation, Mediation and Arbitration
CIP Act	Critical Infrastructure Protection Act 8 of 2019
IT	Information Technology
NKP Act	National Key Point Act 102 of 1980
PSIR Act	Private Security Industry Regulation Act 56 of 2001
PSiRA	Private Security Industry Regulatory Authority
SANDF	South African National Defence Force
SAPS	South African Police Service
SOB	Security Officers Board
SSA	State Security Agency

EXECUTIVE SUMMARY

Critical infrastructures are targeted by various forms of attacks for different motives. This study views an attack towards a critical infrastructure as an attack on the economy, national security, and the state's functioning. For this reason, the protection of critical infrastructures remain crucial. In South Africa, critical infrastructure protection is not a new phenomenon. It dates to the protection of national key points which happened in the late 1970s and early 1980s after the establishment of National Key Point Act 102 of 1980. During the time of the promulgation of that legislation, South Africa was faced with a state of emergency, political turmoil, and violent protests with state resources heavily spent on maintaining the apartheid system of segregation.

Consequently, national key points were left vulnerable, as the state police were overwhelmed by the pressure to quell civil unrest. This led to a withdrawal from certain policing duties, as efforts were redirected towards maintaining state security and political control. This arguably led to the formation of the South African private security industry and its involvement in safeguarding national key points since police were focused on other matters. The National Key Point Act governed all security related activities within national key points. Years later, the National Key Point Act 102 of 1980 was repealed and replaced by a new legislation namely, Critical Infrastructure Protection Act 8 of 2019. Hence the name changed from 'national key point' to 'critical infrastructure'. The new Act was promulgated to mitigate any threats (including criminal acts) directed to the country's critical infrastructures.

The participation of the private security industry in national security underscores the need for PSiRA to bolster its regulatory framework. Inadequate regulation within critical infrastructure protection could potentially allow criminal elements to pose as legitimate security service providers, granting adversaries access to critical infrastructures and leaving them vulnerable to attacks. This qualitative research study, the first of its kind, was undertaken to investigate, evaluate, and enhance the regulatory framework of the private security industry in safeguarding South African critical infrastructures.

The study found that although there is the Critical Infrastructure Protection Act, the protection of critical infrastructures is still regulated by the repealed legislation. The same Act is also used to develop training standards for security service providers and prospective officers in that space. Unlike the National Key Point Act, the new Act grants PSiRA powers to determine and recognise training standards for critical infrastructure protection, which is a new regulatory terrain to be traversed and mastered by the Authority. This study strongly recommends that PSiRA should consider developing regulations for critical infrastructure protection. This would enable the Authority and its stakeholders to identify key areas to be strengthened in the regulation of private security service providers who protect the country's critical infrastructures.



1. INTRODUCTION

The imperative to fortify critical infrastructures against criminal activities resonates worldwide, marking an enduring and ever-relevant topic of discourse. As indicated by Izycki and Colli (2019), the term critical infrastructure has two constituent elements: Firstly, services and facilities used by society (infrastructure); and secondly, their relevance (critical) as measured by the negative consequences of their disruption or malfunction in the public.

It is of the utmost importance to comprehend that critical infrastructures can be privately or publicly owned. Critical infrastructures could be compromised or attacked by different criminals for different reasons. Terrorism is the most prevalent form of criminal attack against critical infrastructures. As noted by Chalk (2008), terrorism is primarily driven by political ambitions with an aim of destabilising the *status quo* and attracting government and/or media attention.

Terrorists have been known to target critical infrastructures as they receive more attention than other structures. An attack on critical infrastructure means an attack on the economy, national security, and state's functioning. Owing to some researchers, the primary goal of terrorism is to destabilise the state's economy through asymmetric warfare (Chalk, 2008 and Tichy, 2019). The most well-known terrorist incident happened in the United States of America on 11 September 2001, prompting several governments to prioritise national security by protecting their critical infrastructures. The history of critical infrastructure protection in South Africa has some similarities to that of other countries, however it has different nuances.

While terrorism is often cited as the primary threat to critical infrastructure security worldwide, various other criminal activities, including targeted ransom demands, pose significant risks to their integrity (Maia, Praca, Mantzana, Gkotsis, Petrucci, Biasin, Kamenjasevic, & Lammari, 2020). Terrorism and ransom crimes are prevalent but strategies for sabotaging critical infrastructures have greatly advanced due to technological innovation.

These criminal attacks are no longer only carried out physically as they were in previous years; they can now be carried out either physically or digitally (cyber), and they are sometimes combined cyber-physical attacks. The goal of these attacks is to undermine national security as well as to generate money. Many governments have developed national physical or cyber security strategies to protect their critical infrastructures against



criminal attacks. Different pieces of legislation, policies, and strategies have been developed in South Africa to deal with any threats against critical infrastructures.

The Critical Infrastructure Protection Act 8 of 2019 (CIP Act) was promulgated to circumvent any criminal acts directed to South African critical infrastructures. The purpose of the CIP Act is clearly stated in section 2. Among other reasons for its establishment was to secure critical infrastructures against any threat. The CIP Act does not only provides measures and mechanisms to be used to protect critical infrastructures; but also makes mention of the role of the private security industry in the protection of these infrastructures. Moreover, the CIP Act recognises the Private Security Industry Regulatory Authority (PSiRA) as the regulator of private security services and providers in that space. The involvement of private security industry in such a highly regulated space necessitates PSiRA to keep up with its regulatory mechanisms to ensure professionalism through effective regulation of the industry.

The lack of effective regulation of the industry has the potential of enabling criminal elements to masquerade as security service providers with an aim to gain access to critical infrastructures thereafter attack them. Hence, the Constitution of the Republic of South Africa stipulates in section 199(3) and (4) that any other security services that are not established in terms of the Constitution may only be established, structured, and regulated in terms of the national legislation. PSiRA, therefore, exists to regulate private security services and to exercise effective control over the practice of the occupation of security service providers in the public and national interest, and in the interest of the industry itself. This simply means that any other private individual or company who is not established in terms of any legislation but offers private security services, or gives an impression of offering such services, shall be subjected to PSiRA regulations. This study covers all 'private' security services rendered in the protection of critical infrastructures (be it physically and/or digitally) and provides recommendations on how they can be effectively regulated.

2. BACKGROUND OF THE STUDY

Global political conflicts have a significant impact on the terrorist attacks that occurred in the United States of America on September 11, 2001 (9/11). Following those attacks, it is argued that countries around the world began to identify infrastructures that could be vulnerable to natural disasters as well as criminal attacks (Mihaljevic, 2018). According to Mihaljevic (2018), these infrastructures are crucial to the ongoing operation of the economy and society; thus, they are referred to as critical infrastructures. Furthermore, critical infrastructure protection remains one of the top national security priorities, serving to safeguard society's core values.

This research highlights the necessity of prioritising the protection of critical infrastructures, a task complicated by the need to analyse the role and contribution of the private security sector. Effectively safeguarding critical infrastructures hinges on understanding the crucial role played by the private security sector in their protection and preservation (Mihaljevic, 2018).

The protection of critical infrastructures in South Africa dates to the Apartheid era, when black liberation movements targeted these critical infrastructures for their voices to be heard. Back then critical infrastructures were known as National Key Points. The National Key Points Act 102 of 1980 governed the protection of National Key Points, which was repealed and replaced by the CIP Act. The latter defines an infrastructure as any building, centre, establishment, facility, installation, pipeline, premises, or systems needed for the functioning of society, the government, or enterprises of the republic and includes any transport network or network for the delivery of electricity or water.

Since these infrastructures are critical to the functioning of the state and society, the Minister of Police therefore has the powers to declare them as critical infrastructures in terms of section 20 of the CIP Act. Mihaljevic (2018) noted previously that extensive attention must be paid to the protection of critical infrastructures, and this cannot be done without the participation of the private security industry.

It is a known fact that the private security industry is profit-driven, and when entrusted with safeguarding the country's critical infrastructures, it must be highly regulated by relevant Authorities. To improve the services rendered by security service providers, the regulator of the industry must identify regulatory challenges in this space. Critical infrastructure destabilisation can take the form of physical or cyber-attacks, and these attacks can originate

within or outside South African borders (Botha, 2020). The regulation of private security services remains critical in national security. Furthermore, it is observed that the political position of South Africa in global politics may soon expose its critical infrastructures to various forms of attacks, and the potential enemy may probably use private security service providers (if they are not effectively regulated), to gain access to these infrastructures. This includes both physical and cyber security service providers hence, their regulation can never be overemphasised.

A security service provider is defined in the CIP Act as one who provides security services as defined in Section 1 of the Private Security Industry Regulation Act 56 of 2001. This means that PSiRA must regulate security services provided by a third party to a critical infrastructure. The research pinpointed that cybercriminals are targeting critical infrastructures, which is a matter of national security (Xulu, 2022). Furthermore, it raised a serious issue of critical infrastructures' cyberspace being protected by unregulated 'private' security service providers, which, according to the study, has the potential to compromise state security, particularly where sensitive information is involved (Xulu, 2022, p. 31). As a result, it is critical to establish regulatory challenges that will not jeopardise national security and develop mechanisms to effectively regulate the industry in critical infrastructures.

It is submitted that private security should not focus only on physical security within critical infrastructures, as their cyber components have emerged as vulnerable targets for exploitation by criminals. Additionally, this study extends beyond physical security and is not solely guided by the CIP Act; rather, it encompasses the protection of critical infrastructures by private security service providers. The study does not differentiate between security services aimed at safeguarding systems essential for societal, governmental, or commercial functions, including transportation networks or utilities, as there is no legislation excluding the protection of these critical infrastructure areas recognised by the CIP Act. Consequently, security services within critical infrastructures encompass both physical and digital aspects, as section 4(2)(c)(ii) of the CIP Act mandates the appointment of a private sector cybersecurity expert by the minister. Hence, private cybersecurity services are included in this discussion.

3. RESEARCH AIM, HYPOTHESIS, OBJECTIVES AND QUESTIONS

The aim of the study is to explore, examine, and strengthen the regulatory framework of the private security industry in the protection of South African critical infrastructures.

The research hypothesis of this study is as follows:

Failure to effectively regulate private security service providers in critical infrastructure may expose the country's security to espionage, which could lead to criminal attacks of any form.

The objectives of the study are to,

- Identify key areas of critical infrastructures that require private security services;
- Establish the effectiveness of regulatory mechanisms used to regulate security services and providers in critical infrastructures;
- Examine the level of adequacy of training provided to security service providers operating in critical infrastructures;
- Uncover the conduct of security service providers in the critical infrastructures; and
- Provide effective regulatory framework for private security industry protecting critical infrastructures.

The primary research question is: *What strategies can be developed to strengthen the regulatory framework of the private security industry in the protection of the country's critical infrastructures?*

The secondary research questions are as follows:

- Which key areas of critical infrastructures require the protection of private security services?
- What are the current regulatory mechanisms used to regulate security services and providers in critical infrastructures?
- Is the level of training provided to security service providers adequate for the protection of critical infrastructures against any form of threats?
- What is the conduct of security service providers in critical infrastructures?

4. RESEARCH METHODOLOGY

This part discusses research procedures or techniques that were employed to identify, select, process, and analyse data about the regulation of private security in critical infrastructures as the study sought to discover the reality about the private security industry in the protection of critical infrastructures. Therefore, the study adopted an interpretivism research paradigm. Thanh and Thanh (2015:24) are of the view that reality is socially constructed, meaning scholars need to acquire more knowledge of the phenomenon being studied through participants' perceptions and experiences. The responses of the research in the interpretivism paradigm are received from experiences of the participants and researchers must construct meanings through interpretation and analysis of the collected data (Thanh & Thanh, 2015:24).

The research method that provided an in-depth understanding of the phenomenon being studied was a qualitative research approach. Creswell (2009:4) defines this approach as a way of exploring and understanding views of the individuals or groups that ascribe to the research problem. The qualitative research approach provided an opportunity for security service providers to relate their experiences in the protection of critical infrastructures. The research used face-to-face and virtual interviews as data collection instruments. The interview questions were semi-structured. Structured sets of questions were developed to allow for follow-up questions where there were unclear statements made by the participants.

The population of the study was in-house and contracted security service providers (including officers, businesses, and training centres). The sample was selected from the population using a purposive sampling method. Tangco (2007:147) defines purposive sampling as a non-random sampling that selects participants according to the qualities they possess. Thematic data analysis was used to analyse the collected data. For validity and reliability of the data collected, a member-checking method was used. Carlson (2010:1105) refers to member checking as a way of finding out whether the data analysis is in line with the participants' experiences.

There were few research limitations identified during the gathering of data. For instance, due to the sensitivity of information that security service providers operating in the critical infrastructure protection environment are exposed to, some were reluctant to share more information about the security of their critical infrastructure. They were concerned that this would compromise the security of both their organization and nearby communities. It is worth noting that research ethics principles emphasize the protection of research participants' rights (Levine, Faden, Grady, Hammerschmidt, Eckenwiler & Sugarman, 2004). Which means that, while security service providers are required by law to comply with PSiRA's regulations, if they are participating in an Authority's research, they are not obliged to respond to any question(s) that they are uncomfortable answering. They must fully enjoy their rights as research participants and the researcher was mindful of that. This should not be interpreted as defying their legal obligation to comply with the Authority's regulations. However, participation in this research was voluntary.

Another limitation of the study was that while some participants were willing to participate, they had to obtain consent from their upper management in advance. Unfortunately, they were unable to obtain that approval until the data collection process was completed. While on the limitation of the study, the researcher also contacted key stakeholders in critical infrastructure protection in South Africa; however, others were unable to participate. An attempt to get hold of the State Security Agency and SAPS (National Key Point Division) was unsuccessful. SAPS, as the custodian of the Critical Infrastructure Protection Act 8 of 2019, would have given more details on this phenomenon. Based on their experiences with private security service providers, they would have provided insight on the effectiveness of their security services, and areas where PSiRA should improve to achieve effective regulation of the industry in that field.

To uphold the confidentiality and anonymity of sensitive information central to the study's focus, written consent forms were crafted. These forms addressed the confidentiality of any information provided. Additionally, access letters seeking permission to conduct interviews were dispatched to selected participants via email.

5. LITERATURE REVIEW

This part discusses the existing literature on the protection of critical infrastructures.

5.1 History of critical infrastructure protection and the involvement of the private security industry

The literature reveals that the idea of protecting critical infrastructures is not a novel phenomenon. Despite the lack of a legal term for 'critical infrastructure protection' at the time, nations all over the world had measures in place to protect their vulnerable areas from threats, whether natural or man-made disasters (Babos, 2016). It was further argued that Egyptian, Greek, or Roman empires alike, protected their transportation networks, food-supply routes, material resources or management techniques and kept them secret (Babos, 2016). Although it was not yet recognised as such, that alone constituted the protection of critical infrastructures. Nevertheless, it is unclear from the reviewed literature who was securing those infrastructures — private citizens or state-affiliated security personnel.

Scholars such as Parfomak (2004), Mihaljevic (2018), and others, deliberately or unintentionally support the myth that the 9/11 attacks made the stringent security of critical infrastructures a popular subject of discussion. This appears to be a scientific falsehood spread to discredit the excellent efforts of many countries that have been protecting their critical infrastructures before the 9/11 attacks. That critical infrastructure protection is not a recent development is accurate, as stated by Babos (2016). For example, in South Africa, national key points were first protected in the late 1970s and early 1980s after the National Key Point Act 102 of 1980 (NKP Act) was established. During this time, it is argued that the country was faced with a state of emergency, political turmoil, and violent protests with state resources heavily spent on maintaining the apartheid system of segregation (Berg & Gabi, 2011). The black liberation movements made a pledge to make the country ungovernable until their demands were met, which mounted pressure on the state police to suppress civil unrest, resulting in the withdrawal of state police from some policing functions to focus on maintaining state security and political control (Berg & Gabi, 2011). Ultimately this led to the formation of the private security industry in South Africa to fill the gap left by the state police. Berg and Gabi (2011) asserted that private security providers, specifically security businesses, were designated to safeguard national key points as stipulated in the Act.

In the late 70s and early 80s when the industry started to protect national key points, there was no regulatory body to regulate the appointed security service providers. The first legislation (Security Officers Act 92 of 1987) to regulate the industry was passed in October 1987 and promulgated in April 1989 (Berg & Gabi, 2011). The Security Officers Act 92 of 1987 was established primarily to create the Security Officers' Board to regulate and professionalise the industry (Berg & Gabi, 2011). In-house security service providers had to wait a decade before they were included in the 1997 amendment of the Security Officers Act. This is a clear demonstration that the apartheid government already had measures in place to protect their national key points against any security threats mainly terrorist's attacks which were politically motivated. The democratically elected government inherited the NKP Act in 1994.

As indicated earlier in the study, the NKP Act was repealed and replaced in 2019 by the CIP Act. Even its replacement was not motivated by the 9/11 incidents, but it was mainly influenced by the new Constitution of the Republic of South Africa. The 9/11 attacks, according to research, mainly affected three sectors which happen to be part of critical infrastructure protection namely, aviation, maritime and nuclear (Parfomak, 2004). Thus, the regulatory framework of security for the three sectors were strengthened worldwide. They even have international standards set and are highly regulated as compared to their counterparts in the water, banking, health etc.

5.2 The protection of critical infrastructures against cyber-threats

The previous part detailed the history of critical infrastructure protection from the standpoint of physical security. This part analyses the role that cybersecurity plays in securing critical infrastructures.

In 1980, when the NKP Act was enacted, cyber threats targeting National Key Points were non-existent. Moreover, computer system usage was not as prevalent as it is today. The increasing dependence of critical infrastructures on interconnected computer systems, vital for sustaining economic growth and societal welfare, has rendered them susceptible to various cyber threats. These threats not only pose risks to critical infrastructures but also have adverse effects on a nation's economy and service delivery (Hurst, Shone, & Qi, 2016; Kim, 2014).

According to Karabacak and Tatar (2014), there are different types of threats with different motivations, qualifications, and capacities. All these threats target specific weaknesses in a critical infrastructure cyber system (Karabacak & Tatar, 2014). The NKP Act did not address cyber-threats, while the current CIP Act states in section 1 that security “includes but is not limited to ‘physical security’ of critical infrastructure.” Furthermore, the Act defines threats as “any actions or omission of a criminal, terrorist, or accidental nature which may potentially cause damage, harm, or loss to the critical infrastructure or interfere with the ability or availability of critical infrastructure to deliver basic public services and may involve any natural hazard which is likely to increase the vulnerability of the critical infrastructure.” This definition encompasses every threat affecting the operation of critical infrastructures, including cyber-threats.

Karabacak and Tatar (2014) argue that in order to cope with threats, vulnerabilities must be mitigated by a critical infrastructure. Cyber war, cyber espionage, cyberterrorism, and cybercrime are examples of such vulnerabilities or threats. There are various solutions available for mitigating these vulnerabilities (Karabacak and Tatar, 2014). South African critical infrastructures employ different types of measures to mitigate cyber-threats. The provision of security services in the country’s critical infrastructures is made up of public security service providers (e.g., the police, military, etc.), and private security service providers (private companies and officers) established, structured, and regulated by the PSIR Act. The importance of regulating cyber security services and their providers is still being debated, as some of the country’s critical infrastructures are protected by “private” cyber security service providers.

According to the Oxford Dictionary, security is “the state of being free from danger or threats.” Moreover, the definition of security or security services in the PSIR Act does not limit security to threats of criminality or specify the environment (physical or digital) in which these threats may arise. Additionally, the Act does not specify the types of threats against which the protected person or property is safeguarded. This lack of specificity implies that the concept of security is broad and may require interpretation to fully grasp its meaning. Therefore, Button (2020) and Xulu (2022) proposed an intriguing argument that the emergence of threats due to organisational practices and society’s reliance on digital platforms, commonly referred to as cyberspace, has given rise to a new concept known as cybersecurity.

The literature provided an example of a cyber war named Stuxnet, which happened in 2010 and was directed at Iranian nuclear energy infrastructure (Karabacak & Tatar, 2014). Most cybersecurity experts contend that the Stuxnet virus reflects the beginning of a serious cyber warfare. The Stuxnet has the potential to attack our security equipment which raises the question of how the Authority would mitigate those threats against security equipment during a cyber-war. These regulatory questions presented by the literature are significant to the security of the country.

5.3 The conduct of security service providers

The code of conduct for security service providers aims to ensure that security service providers obey the law. Hurst *et al.* (2016) argue that the protection of infrastructures includes both internal and external threats, in this instance internal threats include accidents during the working process itself, as well as human caused accidents, theft, sabotage, industrial espionage (Hurst *et al.*, 2016). The external threats being, terrorist attacks, diversions, natural disasters, invasion, among other things. (Hurst *et al.*, 2016). Following the findings of Thoka's (2021) research, which was carried out in one of the country's critical infrastructures namely, Medupi power station. Thoka (2021) discovered that the likelihood of internal workers committing theft was found to be significant due to lack of security control measures. Some security officers were discovered to be conspiring with contract workers to remove cables from the site (Thoka, 2021). According to a participant in Thoka's study, one security officer was discovered stealing without wearing a uniform and disguised as a contract worker. Thus, when evaluating threats and countermeasures for critical infrastructure protection, internal threats should not be overlooked.

5.4 The formation of critical infrastructure protection regulator

In the news article published by BusinessTech (2023), it was pointed out that the civilian secretariat for police service has gazetted new draft regulations for public comment, which aim to establish a new council, the regulator, and a host of new functions for the Minister of Police to protect the country's critical infrastructures. The regulator will be established by the National Commissioner of Police in line with regulation 9 of the Critical Infrastructure Protection Regulations, 2023 (Draft Regulations). It has been noticed that the published regulations place a greater focus on the physical aspects of security, while the cyber aspect of security is not stated explicitly. However, these are draft regulations which are subject to change. As there is no literature about the critical infrastructure protection regulator,

this study would have to clarify its role and mandate in the regulation of security services and providers. The functions of the regulator, according to regulation 9(7)(m), would be to keep records of security service providers who render security services to critical infrastructures. The assumption could be that security services would have to be established, structured, and regulated by a national legislation as stipulated in section 199 of the Constitution. Therefore, the regulatory question of cybersecurity service providers protecting critical infrastructures remains a burning issue.

Critical infrastructure protection is insufficient if there are no regulatory measures in place to deal with internal and external threats. PSiRA, as the national regulator of the private security, is mandated to regulate the private security industry and exercise effective control over the practice of occupation of security service providers in the public and national interest and the interest of the private security industry itself (PSiR Act). The Authority conducted many studies on the regulation of different sectors and security services. Some studies were carried out in areas where security service providers protect critical infrastructures such as airports, ports, railway, cybersecurity, and in-house security. The subject of security training provided to security service providers deployed in critical infrastructures is common to all four studies (airport, maritime, railway, and in-house security). Each sector has its own security training programme and national key point training is required as an additional training.

According to Seanego and Xulu (2020, p. 13), the course contents are mainly focused on the use of different kinds of firearms in these spaces. However, cyber-threats were not included in threats throughout the national key point era. As a result, this training is incompatible with the new CIP Act. Not all threats to critical infrastructures require the use of a firearm; others are as simple as pressing a computer key (Xulu, 2022). Regulation 9(7) (i) specifies that the Regulator would specifically support the National Commissioner in the performance of the functions assigned to him or her under Section 9(3) of the CIP Act and monitor and evaluate the standard of - (i) security at critical infrastructures; and (ii) 'training at training institutions' to address any identified inefficiencies. Therefore, this research examined the level of physical training offered to security officers operating in that sector, as well as how the Authority could contribute to the advancement of the expertise of those security officers (if required).

6. RESEARCH FINDINGS

This section unveils the research findings concerning the involvement of the private security industry in safeguarding critical infrastructures in South Africa. Additionally, it delves into intriguing discussions regarding the regulation of this industry in the context of critical infrastructure protection. These discussions are structured in alignment with the study's objectives.

6.1 The key areas of critical infrastructure protection

The study sought to identify key areas in a critical infrastructure that requires private security service providers' protection. This was derived from section 2 of the CIP Act, which prescribes the primary purpose of the legislation. Among others, the primary aim of the CIP Act is to secure critical infrastructures against any threat. Furthermore, section 24(7) of the Act grants powers and duties to a person in control of a critical infrastructure to appoint a person - in the employ of the critical infrastructure - as a security manager to protect the infrastructure against any security related threats. In the terminology of the Authority, the appointed security manager falls under the category of 'in-house security service provider' since he or she is in the employ of an organisation which is not a 'security business', to manage, control and supervise the rendering of any security services within a critical infrastructure. The in-house security service provider is part of the industry (Xulu, 2020). The appointed security managers are in a strategic position of security in critical infrastructures. This demonstrates that the private security industry plays a significant role in the protection of South Africa's critical infrastructures.

6.1.1 Three crucial areas of critical infrastructures

Since the CIP Act aims to secure critical infrastructures against threats, in particular security related threats, this section uncovers areas where security related threats can emanate from. From the study, it is evident that the protection of critical infrastructures has focused on the protection of the people and physical property. While doing so, the security of the airspace (within the demarcation, jurisdiction, or territory of the critical infrastructure) and cyberspace of critical infrastructures have been overlooked. This means that there are three key areas of a critical infrastructure that requires serious protection namely, (1) physical or ground space (people, and property [moveable and immovable]), (2) airspace, and (3) cyberspace. This study has shown that if any of the three areas can be seriously compromised, the country may witness a catastrophic event. Section 24(7)(a) of the CIP Act stipulates that a security

manager should implement and monitor on behalf of a person in control of the critical infrastructure, the prescribed *security policy and plan* compiled for that critical infrastructure. This research discovered that most security policies and plans drafted in terms of section 9(3)(f) and implemented by the appointed security managers are incomplete simply because they do not clearly specify the protection of the airspace and cyberspace of critical infrastructures.

According to the national design basis threats, our critical infrastructures are more affected by insider threats than outsider threats. Hunker and Probst (2011) define an insider as a person who is deeply embedded in an organisation, highly trusted, and in a position to do great damage if so inclined. This person may have been legitimately empowered with the right to access, represent, or decide about one or more assets of the organisation's structure (Hunker & Probst, 2011). Therefore, an insider threat is posed by an individual with privileges within an organisation who may misuse them or whose access results in malicious acts (Hunker & Probst, 2011). The two scholars also contend that the skills possessed by an insider are a key determinant of the threat they may pose as a malicious insider. For instance, private cybersecurity service providers could be deemed as posing a high risk of insider threats due to their skill sets. Given that cybersecurity is acknowledged as a scarce skill, if cybersecurity practitioners were to decide to engage in malicious activities, it would be challenging for law enforcement agencies to mitigate these actions.

The findings of this study have shown that disgruntled employees are a significant insider threat. Many disgruntled employees have concerns about certain employment conditions such as failure to pay salaries, underpayment of employees, exploitation, unfavourable working conditions, etc. Sarkar (2010) argued that insider threats conjure up images of disgruntled employees planning to take revenge or malicious employees looking for financial gains. This form of threat may affect all security officers who protect key areas of critical infrastructures ranging from physical space (including airspace) to cyberspace.

This research further revealed that due to security measures put in place for the protection of the critical infrastructure's physical space, this space cannot be regarded as the most vulnerable, simply because its protection started a long time ago and the industry has mastered how to secure it. The deployed measures make it difficult for criminals to wage their attacks physically, they may explore other vulnerable avenues to execute their mission if they establish that they cannot attack physically. Those avenues may be either the airspace (airstrikes) and/or cyberspace (cyberattacks).

Given that critical infrastructures belong to various sectors and face diverse threats, it is essential to recognise these distinctions. For example, the petroleum and banking sectors encounter different types of threats. While airspace security may not be a top priority in banking, it holds paramount importance in the petroleum sector. Protecting against cyber threats in the petroleum sector is crucial, albeit not to the same extent as in banking. Nevertheless, this study revealed that criminal elements targeting critical infrastructures focus on consistent areas of interest. Therefore, discussions on critical infrastructure protection should always encompass physical, airspace, and cyber domains.

6.2 The regulatory mechanisms in the protection of critical infrastructures

This part of the research analyses the current critical infrastructure protection laws and their role in ensuring the safety of the country's critical infrastructures.

6.2.1 Shortcomings in the legislation governing critical infrastructure protection

Security operations in the country's critical infrastructures are currently not guided by the CIP Act, they are still under the regulatory realm of the NKP Act which was repealed and replaced by the new legislation. The industry indicated that the South African Police Service (SAPS) is consulting on the draft regulations of the new legislation and the establishment of the critical infrastructure protection regulator. The perception towards the new Act is that its design puts more emphasis on physical security than airspace or cyber security in the protection of critical infrastructures. Many are of the view that the new legislation follows the footsteps of the repealed legislation in the regulation of security services and is oblivious of the evolving world. This has been seen as a regulatory gap simply because the world is becoming more digital and relying more on the physical and cyberspace. It is inappropriate for the legislation, which is aimed at protecting critical infrastructures of the country, to focus more on physical or ground security rather than airspace and cyberspace security. This statement does not mean there are no airspace and cybersecurity measures in place to protect critical infrastructures. The focus, however, is on the regulatory framework in place for those who operate in those spaces. Cybersecurity service providers who were protecting critical infrastructure's cyberspace indicated that the legislation should have specified key areas identified as critical infrastructures in a cyberspace and the regulatory framework for the security services rendered.

a) The critical infrastructure protection regulator and its importance

SAPS would be establishing the regulator of critical infrastructure protection as informed by regulation 8 of the draft regulations. The regulations are developed in terms of section 27 of the CIP Act, which stipulates that the National Commissioner shall establish a critical infrastructure protection regulator within the structures of the SAPS to ensure the maintenance of the administrative systems and procedures necessary for the implementation and enforcement of the Act as contemplated in section 9 of the Act. One needs to clarify that the critical infrastructure protection regulator's mandate has no potential to overlap with that of PSiRA in the regulation of private security service providers. From our observation, the regulator will look at the security threats and measures (given by the security policy and plan) needed to mitigate those threats confronting critical infrastructures. Whereas PSiRA's mandate is to regulate those who render private security services as prescribed by the security policy and plan.

The establishment of the critical infrastructure protection regulator is long overdue when it comes to the affairs of private security and its regulation in the critical infrastructure environment. The Authority has been regulating security service providers rendering services in general without focusing on those who protect critical infrastructures. This does not mean that the Authority has never conducted inspections in a critical infrastructure, however the inspections conducted were coincidental. The CIP Act put an obligation for the appointment of in-house security service providers to manage security affairs. Since they are registered as in-house security service providers within PSiRA, the Authority inspects them as such and not as critical infrastructure providers. There is no category of critical infrastructure in the inspection sheet of PSiRA's law enforcement, hence this research put it as a coincidental inspection. With that said, PSiRA has never conducted an inspection on security service providers in their capacity as critical infrastructure security service providers.

Due to the vastness of the industry and financial constraints, the Authority often fails to reach certain critical infrastructures in the country. However, there is a need to intensify the regulation of security service providers operating in critical infrastructure environments. This focus on regulation by the Authority would greatly benefit the nation and the public at large. Additionally, once there are new measures in place the Authority would be able to improve its security training offered to security service providers rendering services in critical infrastructure environments.

While the establishment of the critical infrastructure protection regulator brings many positives, it also comes with regulatory gaps that need to be addressed. Its focus on physical security threats may not be comprehensive enough, as threats can emerge from various sources, including ground, airspace, and cyberspace. Some threats may not require a physical presence at the facility, making it essential to recognise and address non-physical threats as well. Failure to do so could result in non-compliance of individuals or companies who play a role in protecting air and cyberspace and should be subject to regulatory oversight by PSiRA if they give an impression of rendering private security services.

6.2.2 The regulatory framework of PSiRA

a) Registration

In terms of registration, critical infrastructure security managers raised concerns about the mismatch between the training received by security officers and qualifications that appear on their PSiRA registration profiles. They alleged that some security officers hold the highest qualifications of PSiRA training, but their knowledge does not match the certificate they possess. This, according to security managers, is a regulatory loophole created by PSiRA's absence of evaluation criteria before a security officer or prospective security officer can be registered for a particular grade. It was pointed out that security officers and prospective security officers should demonstrate to the Authority, through a written or verbal assessment, their eligibility to be registered for specific qualifications by passing that assessment. This comes after they have interviewed candidates who have acquired their highest grades, namely, grade A and B. They argue that their interview questions were based on grade C knowledge, but they discovered that many of their interviewees could not provide any response on the required information, for example, radio language.

To security managers this issue is a regulatory crisis since they appoint registered security officers. Their expectations were that since those security officers are registered it means that they have the required knowledge which match their certification. However, most of the security officers were clueless. Hence, some organisations opt to have their own security training academies to re-train all their security officers which is costly to their organisations. They pointed out that the money that is supposed to be addressing other security related matters within the organisation is now fixing what should have been rectified by the regulator before or during the registration process. This regulatory loophole, according to security managers, tarnishes the integrity of security as a profession. They further

compared the security profession with other professions that exist in South Africa, such as the legal, medical, accounting, and engineering professions which have strict regulatory mechanisms. Even though their prospective professionals attended reputable universities in the country, their knowledge is evaluated before they are registered as professionals. This evaluation strategy, according to the industry, should be adopted by PSiRA as one of the methods to professionalise the industry.

b) The regulatory guidelines and inspections for critical infrastructures

The absence of regulatory guidelines for security services rendered in critical infrastructure protection continues to be perceived as a challenge not only for the industry, but also regulatory authorities and has an indirect impact on the regulation of the private security industry. The industry indicated that it would be preferable if PSiRA (with the assistance from the experts of Critical Infrastructure Protection) develop regulations for critical infrastructure security service providers. Since critical infrastructures vary with sectors, the involvement of the critical infrastructure protection regulator would assist PSiRA to capture all regulatory intricacies found in that environment and will intensify the role of the private security industry. Furthermore, the regulations will streamline critical infrastructure security with the industry's norms and standards.

This underscores the importance of establishing the critical infrastructure protection regulations. The regulations should specify the expected level of training for security officers and the accreditation process by professional bodies. They should also outline the frequency and thoroughness of inspections conducted by the Authority, approved security equipment for critical infrastructures, and the remuneration standards for security service providers.

The study discovered that almost all critical infrastructures situated in remote areas of the country are unlikely to get inspected by PSiRA. If they happened to have been inspected, this research revealed that it was merely coincidental as law enforcement units target in-house security service providers and auspiciously critical infrastructures. This study found that they are not targeted based on their importance in securing the country's critical infrastructures.

The findings of this research depict that an inspection conducted in a critical infrastructure should not be one sided, meaning, it should not focus only on in-house security providers in the protection of critical infrastructures, but it should contain both in-house and contracted security service providers

since they work together. Any non-compliance found on either side may compromise the security of the country and therefore, the Authority should ensure overall compliance.

The above discussed practice by the Authority's inspectorate may be fueled by its historical background. The literature revealed that the participation of the industry in the protection of critical infrastructures dates back from the early 1980s, and by then regulators of private security (SOB and PSiRA) were not yet established. The first legislation (Security Officers Act 92 of 1987) to regulate the industry was passed in October 1987 and promulgated in April 1989 (Berg & Gabi, 2011). The first regulator to deal with the industry was established in the late 1980s. The legislation that was governing national key point security activities recognised the regulator of the industry at that time, while the SOB was still maneuvering on how to regulate private security services, it was dismantled and replaced by PSiRA due to other regulatory concerns. Since the inception of national key points, the regulators of security service providers did not have a database of national key points that contracted private security service providers. This cannot be attributed to the current regulatory Authority. However, the Authority needs to rectify this historical oversight by establishing a database of critical infrastructures that make use of private security service providers (in-house or contracted) in South Africa. This does not imply that security service providers who protect critical infrastructures are not registered with the Authority.

The reason for development of the database is that PSiRA does not regulate public security services, and there are critical infrastructures that are solely protected by public security service providers (SAPS and South African National Defence Force [SANDF]) e.g., presidential residences. It would be illogical for the Authority to include critical infrastructures that utilise public security service providers in its list. Therefore, the list of critical infrastructures must be filtered to include only those that rely on private security services. Additionally, when developing the database of critical infrastructures, it should be organised provincially or regionally, as per PSiRA's terminology. This is because when they are structured provincially, it would be easier to compile the database of those who use private security providers. Hence, it would be wise for the Authority to consider tasking its regional management to compile the list of critical infrastructures and forward it to the head office's Information Technology (IT) department. Furthermore, when they are structured provincially the study revealed that it will make it easy for the law enforcement unit to conduct thorough inspections in this sector of security. The findings of this research indicate that it would be prudent for the

Authority to conduct regular inspections of all critical infrastructures in the country that utilise private security service providers to ensure compliance. This proactive approach is necessary to address various regulatory concerns and prevent situations where the security of the country's critical infrastructures could be compromised due to non-compliance.

The issue of security companies underpaying or neglecting to pay their employees, as highlighted in previous sections of the study, poses a significant threat to critical infrastructure. This situation could prompt security officers to resort to illicit activities, thereby jeopardizing the security of the properties they are tasked to protect. For instance, consider the scenario where security officers at a critical infrastructure were not receiving their agreed-upon salaries yet remained silent about the exploitation. If these disgruntled security officers were to decide to sabotage the critical infrastructure, it could lead to a national crisis. This underscores the vital importance of conducting regular inspections in critical infrastructures to prevent any potential catastrophic events that could compromise the security of the State.

c) Security equipment and technology

This study discovered a significant shortfall in the regulation of security equipment by the Authority which has the potential to affect the security of critical infrastructures during interstate warfare. The private security industry is the largest distributor of security equipment in that space. Section 35(s) of the PSIR Act states that the Minister may make regulations relating to manufacturing, importation, selling, distribution, and possession of security equipment. The shortcoming identified is the absence of the vulnerability assessments criteria for security equipment used in the rendering of security services before their importation or distribution. The study revealed that security equipment used in the protection of critical infrastructures is not evaluated by engineers who can tell if the equipment and installed technology may infringe the rights of citizens, or if it has been bugged. This is viewed as the gap which can be exploited by criminals. A loophole in security measures is a threat to critical infrastructure, because equipment can be used to capture and send signals to a third party without the knowledge of the onsite security officers.

The previous assertions may sound illusionary; however, it is important to note that the President of the United States of America, Joe Biden indicated that, "I find that the use of Chinese surveillance technology outside the PRC and the development or use of Chinese surveillance technology to facilitate repression or serious human rights abuse constitute unusual

and extraordinary threats,” (Nikkei, 2021). These articulations by the US President led to his government banning 59 Chinese companies due to suspected ties with the defense or surveillance technology sector of China. Among the banned companies, is the largest distributors of security equipment to South African critical infrastructures, known as Hikvision and Dahua (Nikkei, 2021; Pawson, 2023).

According to Pawson (2023), the United States blacklisted both companies due to their technology. It is believed that Hikvision security software and technology provides facial recognition, speech monitoring, and other features. The vulnerability in this is that it becomes intrusive and compromises people’s privacy. There are many factors that contributed to these brands being blacklisted, but it was all due to their innovative technology (Pawson, 2023). If their software is hacked, hackers might have access to whatever security cameras hear and see, which poses a threat to national security (Pawson, 2023). Given the political beliefs of the two countries, one may argue their political ideologies contributed in one way or the other to the prohibition of those security companies. This means that the role of world politics should be always observed when dealing with critical infrastructure protection. Hence, screening of security equipment by the Authority can never be overemphasised.

6.2.3 The regulatory approach for private sector stakeholders

The security of critical infrastructures is composed of various stakeholders with the private security industry and SAPS in the lead. The research revealed that the leading stakeholders in the protection of their cyberspace is the State Security Agency and private cybersecurity companies. This simply means that the protection of critical infrastructures has both the public and private security service providers as key role players. The private sector is the leading stakeholder in both the cyber and physical space of security. However, the regulatory approach differs when it comes to the security services rendered in both spheres.

In the physical space, the CIP Act recognises security service providers who are established and regulated by PSIR Act and report directly to the security managers as stipulated in section 24(7) of the CIP Act. However, with security service providers who operate in the critical infrastructures’ cyberspace, the legislation is silent on how their services can be structured and regulated. They operate in a regulatory vacuum where they are not professionally established. It is worth noting that cyberspace is borderless which makes it difficult for States to mark their territories. This does not mean that they should appoint service providers who are not recognised by

their national legislation to protect the hearts of their countries. A critical infrastructure is the heart of the country, should anything bad happen to it the public suffers the consequences. Therefore, it is a sensitive space.

When one claims that cybersecurity companies are not regulated the statement refers to the industry's professionalisation. Currently, cybersecurity companies cannot be recognised as professional security service providers in terms of the South African law since they are not granted any certification of operation by a regulatory Authority established in accordance with national, regional, or international legislation. Borderless cyberspace means the certification should be recognised by States. Many cybersecurity companies rely on qualifications and experience to demonstrate their capabilities for rendering cybersecurity services. Critical infrastructures engage in a vetting process when appointing private cybersecurity companies, primarily focusing on criminal background checks. However, there are professional issues that may not constitute criminal offenses but are still considered improper conduct within the industry. For instance, insider threats or disgruntled cybersecurity officers may switch companies without their minor misconduct being known, even though it does not amount to a criminal offense. Therefore, regulating cybersecurity service providers is crucial for the industry, state, and public interest.

6.2.4 The appointment of cybersecurity management

In most critical infrastructures, security managers are not aware of measures put in place for the protection of cyberspace. It is alleged that the security of cyberspace resides with people who are neither appointed nor trained to render any security services in terms of the legislation. Those people are the heads of IT departments. The CIP Act makes no provision for the appointment of heads of IT departments to implement and monitor the security policy and plan of security services rendered in cyberspace. This demonstrates a regulatory crisis when security managers, appointed in terms of section 24(7) of the CIP Act to implement and monitor the prescribed security policy and plan compiled for the critical infrastructure, are not aware of the prescribed policy and plan for the protection of the critical infrastructure's cyberspace which is under their protection. What makes matters worse is the appointment of private "security" companies to secure the cyberspace of critical infrastructures, none of the appointed security companies are established and regulated by a national legislation as stipulated in section 199(4) of the Constitution of the Republic, and those companies report directly to IT departments. This requires a legal justification as to why the security detail of one sphere of critical infrastructure protection is managed by a person who is not appointed to manage security matters in

terms of the CIP Act. For example, if criminals or adversaries tamper with physical security equipment deployed to protect a critical infrastructure and cause serious damage physically, the onus will be on the security manager to provide details as to what transpired. If it has been established that criminals tampered with the security system, the IT specialist will be called upon to explain. However, they will not be the first to be contacted. The first point of contact will be a security manager established in terms of section 24(7) of the CIP Act.

6.2.5 The empowerment of locally owned companies

It has been observed that certain state-owned entities classified as critical infrastructures, as per section 20(1) of the CIP Act, often specify requirements in their tenders for securing their digital or cyberspace that make it difficult for South African companies to compete. Consequently, foreign companies with the necessary tools end up securing these tenders. While it is understandable that high-caliber equipment is required for safeguarding critical infrastructures' cyberspace, entrusting this responsibility to foreign security companies raises concerns about their alignment with the interests of the country and its citizens.

If locally-owned cybersecurity companies are not empowered to protect critical infrastructures' cyberspace, the country may face significant challenges in the future. As highlighted in recent studies on the private security industry, the PSIR Act should regulate private cybersecurity services to ensure their structure and oversight. Failure to regulate these services may leave the country vulnerable during interstate cyberwarfare. While security service providers recognised by the CIP Act are regulated by the PSIR Act, cybersecurity service providers operating within critical infrastructures are not subject to the same regulatory framework.

6.3 The level of adequacy of security training

Training offered to security service providers that protect critical infrastructures is adequate to a certain degree because they are able to protect facilities. However, the training needs to be revised and aligned to the CIP Act, because the NKP Act was repealed. Training carried out using the curriculum of the repealed legislation can be viewed as outdated training. For instance, section 2(a) of the CIP Act states that the purpose of the Act is to secure critical infrastructure against threats. This study has shown that security threats can emanate from three distinct areas, ground, airspace, and cyberspace. The modus operandi of an enemy may target one or more of those areas when attacking a critical infrastructure.

Training security service providers solely in physical training and firearm usage is unrealistic many attacks can be carried out remotely without the need for physical presence. For instance, cyberthreats require only a click of a button to potentially disrupt the entire operation of a critical infrastructure. In such cases, even heavily armed onsite security officers would be rendered ineffective. Additionally, certain threats may arise from the failure of security equipment to detect them, such as drones. Therefore, the curriculum of new critical infrastructure protection training must encompass all dimensions of security, despite potential differences in the target market.

According to section 27(m) of the CIP Act, the Minister may, by notice in the Gazette, make regulations in respect of security personnel, including a security manager. These standards and training courses may be determined and recognised by the Private Security Industry Regulatory Authority (PSiRA) which security personnel in the critical infrastructure space must comply with. This means that the Authority has a mandate to determine and accredit the security training received by security officers who protect critical infrastructures. During the development of the training standards, the Authority should ensure that the three key areas of critical infrastructure that require protection identified by this study are taken into consideration. These areas warrant distinct training curricula. For example, areas such as cyberspace and airspace could not be treated as physical or ground space when it comes to security. The tactics used to secure these areas are different thus the developed training would require a different approach. Physical fitness and the use of firearms could be necessary in ground security due to the nature of their operations. However, the training strategy for those who operate in the airspace or cyberspace would not need physical and firearm training but different training standards all together.

As alluded earlier, security officers are still trained using the old curriculum. The previous legislation did not put PSiRA at the centre of training for security personnel who protect those spaces. However, as indicated in the above paragraph the Authority has the role to play in the training of those professionals. There are many concerns raised about the security training which is currently offered by the Authority to security officers. The industry indicated that the point of departure for the Authority is to accept the fact that grades are far from being relevant in critical infrastructure protection training. The concern raised about training received by officers was, firstly, that the training is based more on theoretical learning than practical. The industry indicated that when a security officer is deployed in a critical infrastructure they need to be physically fit. Their operations need a lot more tactical training than theory.



Secondly - mental fitness is another crucial aspect that must be addressed. While the Authority may not have the ability to alter an individual's mental state, it is essential to implement measures during security and critical infrastructure protection training enrolment. This may include conducting psychometric tests to assess candidates' mental fitness.

Thirdly, the current training provided to security officers lacks coverage of the technological aspects prevalent in the industry. As nearly all critical infrastructures are now digitally connected, there exists a regulatory gap in terms of security standards. PSiRA's regulations have been criticised for this shortfall, prompting recommendations for the Authority to offer basic training in security technology. Additionally, training instructors responsible for educating personnel protecting critical infrastructures face challenges in registering as moderators or assessors within PSiRA's system, as they are unable to add these services.

This research found that cybersecurity service providers who protect critical infrastructure's cyberspace against security threats are not equipped with critical infrastructure protection training because there is no security training given to cybersecurity personnel that protect such spaces in South Africa. This challenge should be viewed as an international regulatory crisis since cyberspace is borderless. Since it has been identified that the national key point training does not cover that area of security, the Authority should consider ensuring that when security training is developed, those who protect South African critical infrastructure's cyberspace are also trained in critical infrastructure protection.

6.3.1 Training of currently registered security service providers in cybersecurity

Some participants suggested that currently registered security service providers should be trained to offer cybersecurity services. However, training security officers in cybersecurity services would be unlawful unless those services are regulated by a professional body established under national legislation. This would violate section 4(k)(v) of the PSiR Act, which mandates the Authority to determine and accredit qualifications required for specific security services. The regulatory dilemma lies in identifying who, other than PSiRA, would accredit cybersecurity training for cybersecurity service providers, and under which legislation. If PSiRA lacks authority to accredit cybersecurity services, then training providers cannot legally train registered security service providers in cybersecurity services, as it would contravene section 4(k)(v) of the Act.

It is worth noting that physical security and cybersecurity are two distinct fields that exist in two separate worlds and cannot be integrated. The closest cybersecurity training that physical security service providers could be trained on is, cybersecurity awareness, because it will allow them to detect when their physical security equipment has been tampered with. When they extend their services to protect the cyberspace of critical infrastructures, it would result in a regulatory disaster for not only the Authority but the security of the country. Cybersecurity is a highly sophisticated industry with its own security service providers and regulatory loopholes. Therefore, this study has shown that the industry should not be encouraged to extend their offering to cybersecurity services until there is a regulatory authority to govern those services.

6.3.2 The involvement of (un)educated security personnel in the training industry

This study revealed that if PSiRA intends to establish high standards in the critical infrastructure protection training for security service providers and prospective security service providers, the Authority should begin to advocate for education in the industry by ensuring that everyone who desires to work in this sector should have a minimum of a matric certificate. Professionalisation of the industry lies within the training sector, until that sector is properly regulated, professionalisation of the industry will remain an unattainable objective for the Authority. A question was raised, "How does PSiRA accept directors of training centres who do not have matric certificates to have security training businesses?". The argument is that in other sectors of the industry, security personnel without matric certificates

could participate but allowing non-matriculated security officers to open training businesses in the name of transformation compromises the industry's professionalisation. If any person (including registered security officers) is interested in the education and training sector, he or she must demonstrate passion for education.

The government has provided many possibilities for historically disadvantaged people who were passionate about education to better themselves. There were programs such as Adult Basic Education and Training (ABET) that sought to give historically disadvantaged persons the opportunity to complete their education. It is considerably worse for young people born after democracy to enter the training sector without a matric certificate. Those young people have no justification for not completing matric. Thus, this issue should be debated within the private security training sector to reach a consensus. If the Authority does not allow this debate to take place, the industry will struggle to attract educated youth. Young people will continue to view the South African private security industry as a solution to their temporary unfavourable economic status, rather than a career path.

6.4 The conduct of security service providers in critical infrastructures

One of the objectives of this research was to acquire knowledge about the conduct of private security service providers who secure critical infrastructures. Thus, this part of the study looks at the significance of the code in critical infrastructure protection as well as the commonly witnessed conduct of security service providers.

6.4.1 The importance of the code of conduct in critical infrastructures

Among other objectives of the Authority is to promote a legitimate and professionalised industry, which acts in terms of the principles contained in the Constitution of the Republic and other applicable law. This can be achieved through security professionals abiding to the code of conduct of the private security industry. If a security service provider's action is not in line with the applicable laws of the country, it means the service provider's conduct is unprofessional, and the Authority would have to intervene and uproot the unethical conduct. PSiRA encourages the industry and other members of the public to report any non-compliance. The aim is to unearth unscrupulous security service providers within the industry. If they are not dealt with, they can compromise the image of the industry and that

of the Authority. Furthermore, the interest of the consumers of security services could also be compromised. Hence, Kempen (2022) argued that doing business with unregistered security providers who are not in good standing with PSiRA, poses various risks to the client and public in general. Therefore, PSiRA must regulate the industry and exercise effective control over the practice of the occupation of security service providers in the public and national interest and in the interest of the industry itself.

This study has shown that if security service providers employed by critical infrastructures are not effectively regulated, they stand a chance of being employed or sourced by clients in other institutions and continue to perpetuate unethical conduct. Consumers of security services would appoint a security service provider based on their work history which shows that they were working for a reputable critical infrastructure. They may not be aware that the service provider was dismissed if there are no effective regulatory mechanisms in place. While this may advantage unscrupulous security service providers it poses a real threat to the consumer of security services as argued by Kempen (2022). Moreover it may disadvantage compliant service providers who do not have the history of protecting critical infrastructures. This constitutes an unfair practice and the Authority would have to protect the interest of the public and that of the industry by ensuring that all security service providers act in accordance with the law. This will be done by enforcing the code of conduct for the private security industry.

6.4.2 Conduct of security service providers

This research revealed that the overall conduct of security service providers who protect South African critical infrastructures is aligned with the industry's code of conduct. However, there is a minority that is still engaging in illicit activities. As Thoka (2021) alluded in the literature section; some dishonest service providers are involved in criminal activities when entrusted with a legal duty to protect and serve. The findings of this study revealed that some security officers are engaged in illicit activities such as stealing from their clients. Some steal copper cables while others leak sensitive documents of critical infrastructures that are not supposed to be leaked to other parties e.g., the media. According to Nkwana (2015, p. 115), this practice is highly influenced by lack of security control measures.

The study found that when dishonest security service providers are dismissed, their employers do not report the dismissal to the Authority. Employers indicate that the challenge they encounter is that employees have rights and when they dismiss them, they should be mindful of those rights.

Security officers have the right to contest any dismissal if they believe it was unfair from the Commission for Conciliation, Mediation and Arbitration (CCMA). It was pointed out that the process may take one to three years depending on the case. Employers indicated that they sometimes wait for contestation of the dismissal before they report to the Authority. In other times, a security officer would not contest the dismissal, and the employer would still fail to report the matter to the Authority.

In an instance where a dismissal is contested, they wait for the process to be concluded since their decision to dismiss a security officer can be overturned by the CCMA. They argued they do not rush to report dishonest security officers to PSiRA, because if a security officer wins the case at CCMA and they discover that the Authority has already withdrawn their registration they may be sued by the same security officer. Section 26(1) of the PSIR Act empowers the Authority to investigate before any suspension or withdrawal of registration. This section of the Act enables PSiRA to hear arguments presented by both parties before a decision is taken.

The Authority must encourage security managers of critical infrastructures to promptly report any misconduct by security officers. Failure to address such misconduct could result in unscrupulous officers being hired by other security companies, potentially leading to theft and loss of clients. Reporting such incidents is crucial to prevent further misconduct. While the CCMA may overturn dismissal decisions if proper procedures were not followed, this does not absolve the officer of their wrongdoing. Once PSiRA withdraws their registration, they cannot be reemployed as security officers. Therefore, critical infrastructures must trust the PSiRA process when dealing with security service providers.

Some security officers have reported not receiving remuneration for up to six months, a concerning misconduct observed by security businesses operating within critical infrastructures. Despite signing contracts promising payment for their services, these security companies are violating South Africa's labour laws, posing a threat to critical infrastructures. The non-payment of salaries may lead security officers to sabotage facilities in protest. Therefore, addressing salary issues in critical infrastructures is paramount for the Authority.

Another misconduct on the rise among security officers in critical infrastructures is misrepresentation. Some officers are reportedly submitting fraudulent sick notes to take unauthorised leave. This practice disrupts daily security operations and may compromise facility security. Security managers often have to call in off-duty officers to cover shifts, resulting in additional costs for the company. Many officers engaging in such conduct have been dismissed as a result.

Additionally, this study found that many in-house security officers responsible for managing security equipment sub-units within critical infrastructures were not registered with PSiRA. Some were unaware of their obligation to register with the Authority, particularly those involved in installing and repairing security equipment.

6.4.3 The implications of cybersecurity professionals' lack of a code of conduct

This study identified critical infrastructure's cyberspace as one of the key areas that requires protection, and those who protect that space must be subjected to the regulation of professional bodies. However, this study uncovered that there is a huge regulatory crisis within the cybersecurity industry because incompetent cybersecurity service providers cannot be blacklisted. While we acknowledge their expertise in the field, every industry has its share of service providers who take risks. Without regulation, critical infrastructures may unwittingly appoint a service provider with a poor reputation and unknown incompetency. While cybersecurity service providers may possess the necessary certification, experience, and tools, their conduct is equally crucial.

Critical infrastructures' cyberspace is in the hands of domestic and international service providers who are not recognised and regulated by any professional body established in terms of any legislation (either domestically, regionally, or internationally). Service level agreements and vetting conducted by the State Security Agency (SSA) cannot be regarded as a form of regulation for cybersecurity service providers simply because even PSiRA registered security service providers are subjected to the same vetting process. Cybersecurity services need to be established, structured, and regulated by a national legislation as stipulated in section 199(3) and (4) of the Constitution. This is a serious regulatory loophole for security of critical infrastructures which needs to be rectified.

6.4.4 Deployment of foreign nationals within critical infrastructures

The prevalence of using unregistered foreign nationals which is commonly reported within the private security industry has now spread to some critical infrastructures in the country. There were security managers who indicated that some security companies smuggle unregistered foreign nationals to protect critical infrastructures during night shifts. It came to the attention of security managers, and they terminated the contract with those unscrupulous security service providers. This prompted the industry to raise concerns about the involvement of foreign nationals in the protection of critical infrastructures. They argued that regulatory authorities should have a debate about the exclusion of foreign nationals in the protection of the country's critical infrastructures.

According to critical infrastructure security managers, foreigners (whether they are in the country legally or illegally) should not be entrusted with the duty to protect South African critical infrastructures. They argued that they were aware that section 23(a) of the PSIR Act which allows permanent residents (documented foreign nationals) within the industry and emphasised that they could be afforded an opportunity to participate in sectors of the industry other than critical infrastructures.

Among other reasons raised about their exclusion is that foreign nationals cannot be trusted in a situation of conflict between South Africa and their country of birth. The industry pointed out that how could one be assured that they will not leak the information to the opponent. Although that is not PSiRA's regulatory purview, it was argued that regulatory authorities should deliberate on such matters. The Authority can only deal with unregistered security service providers that are employed in the protection of critical infrastructures since it constitutes an improper conduct. However, through its knowledge dissemination channels (such as stakeholder engagements and other committee meetings, seminars, webinars, conferences) the discussion about the involvement of foreign nationals in critical infrastructure protection would have to be put forward for further engagement.

7. RECOMMENDATIONS

Effective regulation of private security services remains crucial for maintaining the security of critical infrastructures. This section makes recommendations for ensuring that the Authority and other regulatory authorities effectively regulate private security service providers who protect critical infrastructures.

7.1 Regulation of cybersecurity personnel and companies

Cyberspace is a key area of a critical infrastructure that requires maximum security. Section 1 of the CIP Act states that security personnel or security service provider means any person or service provider registered in terms of section 21 of the PSIR Act. This means all security personnel including cybersecurity personnel should be subjected to certain regulatory standards. Once cybersecurity service providers report directly to a security manager (as discussed above), they will also be obliged to register with PSiRA as security service providers as stated in section 1 of the CIP Act. Hence the need for the regulation of this industry can never be overemphasised.

7.2 Registration of critical infrastructure protection

PSiRA must compile a list of registered critical infrastructure security service providers, ensuring no provider operates without proper registration. Before registration, providers must complete critical infrastructure protection training with a PSiRA-accredited institution.

All providers trained in national key point training must undergo a refresher course in critical infrastructure protection before registration. Those with work experience in critical infrastructure need not to undergo evaluation assessment. However, individuals with national key point training but no critical infrastructure experience must pass an evaluation test for registration.

Training providers offering national key point training seeking accreditation for critical infrastructure protection training must apply for recognition of prior learning from PSiRA. Directors, instructors, and assessors must also complete a refresher training in critical infrastructure protection.



7.3 Establishment of database for critical infrastructures

Establishing a database of critical infrastructures that employ private security service providers is an important step towards effective regulation of the industry within critical infrastructures. PSIRA should task its regional management to develop lists of critical infrastructures that make use of private security services in their areas of responsibility. Once a database has been developed, the Authority must ensure that any critical infrastructure that registers with SAPS and employs private security services be added to the list. This means that our regional offices should work with SAPS to compile a list of newly registered critical infrastructures in the region.

7.4 Development of regulations for critical infrastructures

The Authority should advise the Minister in terms of section 4(c) of the PSiR Act to develop regulations for security services rendered within critical infrastructures. The regulations should cover all aspects pertaining to the safety and security of critical infrastructures. The proposed regulations should incorporate both in-house and contracted security service providers who protect critical infrastructures. Additionally, the regulations should delineate the oversight of private cybersecurity services within critical infrastructures and designate the responsible professional body for regulation.

7.5 Inspections of critical infrastructure security services

Once the database of critical infrastructures has been established, the Authority should make it mandatory for inspections to be conducted monthly at every critical infrastructure in a country. The inspections should not only target in-house security service providers but also include contracted security service providers. Once an inspection has been conducted in a critical infrastructure there should be no area left uncovered. The detailed inspection should include employee background checks and for security managers and directors of security businesses, lifestyle audits should be conducted. Since, this is a matter of national importance, the executive of the Authority would have to be made aware of the state of compliance and any regulatory improvement to be made within critical infrastructures monthly.

The Authority has a responsibility to protect the interests of security service consumers. This study uncovered the alarming ease with which substandard security equipment, some even containing spying software, enters the market, posing significant risks to national security. To tackle this issue, it is recommended that PSiRA establish a specialised unit for security equipment engineers within its law enforcement division. These engineers would assess the integrity of security equipment and software before they are imported or distributed to end users. Given that critical infrastructures often rely on security equipment from providers flagged as high-risk elsewhere, PSiRA's approval of such equipment before its availability in South Africa is crucial to safeguard consumers.

7.6 The establishment of a committee

PSiRA should consider establishing a committee which will advise the Authority on matters relating to critical infrastructure protection. This committee should have representation from critical infrastructure protection, PSiRA representatives and other stakeholders identified to discuss any matters relating to PSiRA regulations in the critical infrastructure protection environment. The representation of PSiRA departments and identification of other stakeholders would have to be determined by the Executive of the Authority.

7.7 Development of training for critical infrastructure protection

In terms of Section 27(m)(ii) of the CIP Act, PSiRA has the mandate to determine and recognise training standards for any security course provided to security personnel including security managers who render security services in a critical infrastructure. The nature of critical infrastructure training, which must be developed by the Authority, would have to cover all three crucial areas of a critical infrastructure, physical (land), airspace and cyberspace. The training for physical security service providers would have to encompass rigorous and intensive physical training, mental fitness, weapon and strategic training.

The Authority should make psychometric assessments mandatory for all security officers seeking critical infrastructure protection training prior to enrolment. These assessments should be conducted by accredited providers recognised by the Health Profession Council of South Africa (HPCSA). Additionally, the Authority should develop compulsory evaluation assessments for both current and prospective critical infrastructure security personnel to ensure the ongoing quality of training. These assessments should be administered to all prospective critical infrastructure security personnel before their registration with PSiRA.

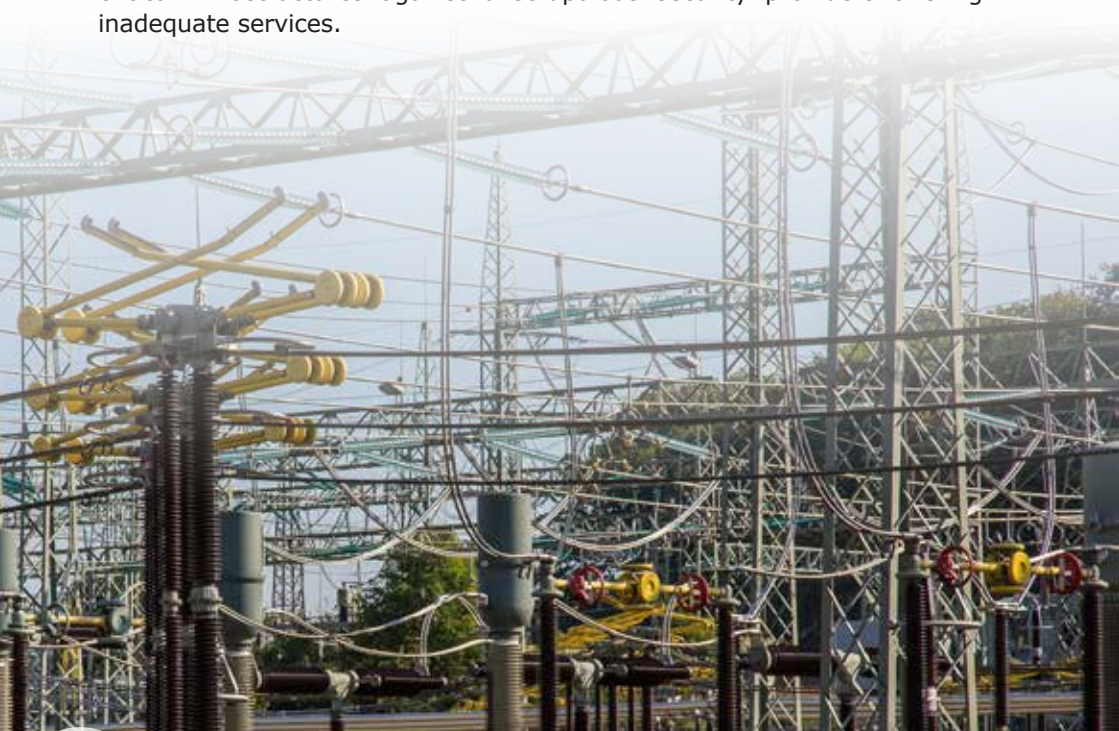
In terms of the standards for training of airspace and cyberspace security personnel, the Authority would have to engage experts in the fields before the development of those standards. It must be noted that every security service provider who protects a critical infrastructure must have completed a course accredited or recognised by PSiRA before they render any security services in the critical infrastructure environment. Therefore, cybersecurity service providers would have to comply with PSiRA's training regulations before they operate in a critical infrastructure. PSiRA as informed by section 27(m)(ii) should determine a cybersecurity course for private cybersecurity service providers who protect critical infrastructure's cyberspace before they operate.

8. CONCLUSION

This study highlights numerous regulatory considerations that PSiRA should consider, particularly those relating to the security of critical infrastructures, which are vital to any country. Given that private security service providers are responsible for safeguarding these infrastructures, strict regulation is imperative.

The absence of robust industry regulations poses a significant risk to national security, as it could allow criminal elements to pose as legitimate security providers and exploit critical infrastructures. Therefore, the aim of this qualitative research was to explore, analyse, and enhance the regulatory framework governing the private security industry in South African critical infrastructure protection.

Adherence to various pieces of legislation governing critical infrastructure protection is crucial for security service providers. Failure to regulate them properly under the relevant laws may expose the country to espionage and potentially catastrophic events. This underscores the vital role of the Private Security Industry Regulatory Authority in safeguarding critical infrastructures against unscrupulous security providers offering inadequate services.



REFERENCES

- Bodnar, J., n.d. Briefing Paper 313: The Private Security Industry. Available at: <https://cplo.org.za/wp-content/uploads/2013/03/BP-313-The-Private-Security-Industry-Dec-2012.pdf>
- Botha, A., 2020. Prevention of terrorist attacks on critical infrastructure. *Handbook of terrorism prevention and preparedness. The age: ICCT Press Publication*, pp.867-896.
- BusinessTech., 2023. New laws to try stop criminals from tearing South Africa apart. Available at: <https://businesstech.co.za/news/government/707478/new-laws-to-try-stop-criminals-from-tearing-south-africa-apart/>
- Chalk, P., 2008. *The maritime dimension of international security: terrorism, piracy, and challenges for the United States* (Vol. 697). Rand Corporation
- Cresswell, J. W. (Ed.), 2009. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). Los Angeles: Sage.
- Critical Infrastructure Protection Act 8 of 2019.
- Critical Infrastructure Protection Regulations., 2023. Invitation for Public Comments: Critical Infrastructure Protection Regulations, 2023. Gazette No: 49045. Available at: https://www.gov.za/sites/default/files/gcis_document/202307/49045gon3732.pdf [Access on 20 July 2023]
- Direnzo, J., Goward, D.A. and Roberts, F.S., 2015, July. The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE.
- Hunker, J. and Probst, C.W., 2011. Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 2(1), pp.4-27.
- Hurst, W., Shone, N. and Qi, S., 2016. CRITICAL INFRASTRUCTURE TESTBED FOR CYBER-SECURITY TRAINING AND RESEARCH (4).
- Izycki, E. and Colli, R., 2019, July. Protection of critical infrastructures in national cyber security strategies. In *ECCWS 2019-Proceedings of the 18th European Conference on Cyber Warfare and Security*.
- Karabacak, B. and Tatar, Ü., 2014. Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. *Critical Infrastructure Protection*, 116, p.63.
- Kempen, A., 2022. Choosing a private security provider Consider the legalities. *Servamus Community-based Safety and Security Magazine*, 115(3), pp.16-17.
- Kibbe, J.D., 2011. Conducting shadow wars. *J. Nat'l Sec. L. & Pol'y*, 5, p.373.
- Kim, D.Y., 2014. Cyber security issues imposed on nuclear power plants. *Annals of Nuclear Energy*, 65, pp.141-143.
- Kothari, C.R., 2004. *Research methodology: Methods and techniques*. New Age International.
- Levine, C., Faden, R., Grady, C., Hammerschmidt, D., Eckenwiler, L. and Sugarman, J., 2004. The limitations of "vulnerability" as a protection for human research participants. *The American Journal of Bioethics*, 4(3), pp.44-49.

- Maia, E., Praça, I., Mantzana, V., Gkotsis, I., Petrucci, P., Biasin, E., Kamenjasevic, E. and Lammari, N., 2020. Security challenges for the critical infrastructures of the healthcare sector.
- Malatji, M., Marnewick, A.L. and von Solms, S., 2020. Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa. *Sustainability* 2021, 13, 291. *Wastewater Based Microbial Biorefinery for Bioenergy Production*, p.171.
- Mihaljević, B., 2018. Protection of critical national infrastructure: challenges for the private security sector. *Annals of Disaster Risk Sciences: ADRS*, 1(1.), pp.47-56.
- Nikkei., 2021. US-CHINA Tensions: *US Releases list of 59 banned Chinese defense and tech companies.*, NikkeiAsia. Available at: <https://asia.nikkei.com/Politics/International-relations/US-China-tensions/US-releases-list-of-59-banned-Chinese-defense-and-tech-companies>
- Pawson, S., 2023. Hikvision & Dahua Blacklisted in U.S.: What Does This Mean For South African Consumers? Available at: [https://activemotion.co.za/hikvision-dahua-blacklisted-in-u-s-what-does-this-mean-for-south-african-consumers/#:~:text=In%20October%202019%2C%20The%20U.S.,selling%20Hikvision%20and%20Dahua%20products](https://activemotion.co.za/hikvision-dahua-blacklisted-in-u-s-what-does-this-mean-for-south-african-consumers/#:~:text=In%20October%202019%2C%20The%20U.S.,selling%20Hikvision%20and%20Dahua%20products.). [Accessed on 01 February 2023].
- Private Security Industry Regulation Act 56 of 2001.
- Sarkar, K.R., 2010. Assessing insider threats to information security using technical, behavioural, and organisational measures. *Information security technical report*, 15(3), pp.112-133.
- Seanego, T. and Xulu, H., 2020. For the love of flying: Exploring the regulation of security service providers in South African Airports. Available at: [https://www.psira.co.za/dmdocuments/research/2021/PSiRA%20Report%20Airport%2001%20\(003\).pdf](https://www.psira.co.za/dmdocuments/research/2021/PSiRA%20Report%20Airport%2001%20(003).pdf) (Accessed: 10 July 2021).
- Thanh, N.C. and Thanh, T.T., 2015. The interconnection between interpretivist paradigm and qualitative methods in education. *American Journal of Educational Science*, 1(2), pp.24-27.
- Thoka, E.M., 2021. *An evaluation of security threats and vulnerabilities to a national key point: case study of Medupi Power Station* (Doctoral dissertation).
- Tichý, L., 2019. Energy infrastructure as a target of terrorist attacks from the Islamic state in Iraq and Syria. *International Journal of Critical Infrastructure Protection*, 25, pp.1-13.
- Tongco, M.D.C., 2007. Purposive sampling as a tool for informant selection. *Ethnobotany Research and applications*, 5, pp.147-158.
- Xulu, H., 2020. Narrowing the Gap: The regulation of in-house security sector in South Africa. Available at: <https://www.psira.co.za/publicity/research.html>
- Xulu, H., 2022. The New Private Security: Regulating Cybersecurity Services in South Africa. *Innovation*, 4, p.10.s



PSiRA
Private Security Industry Regulatory Authority

420 Witch-Hazel Avenue
Eco Glades 2 Office Park
Highveld Ext 70
Centurion
0158


Tel: 086 10 **PSIRA** (77472)

Email : info@psira.co.za

Website: www.psira.co.za

 082 803 4329

 Private Security Industry Regulatory Authority

 Psiralive



PSiRA
Private Security Industry Regulatory Authority



THE PRIVATE SECURITY
in the Protection of South African
Critical Infrastructures

SAFER HOMES
BUSINESSES
COMMUNITIES

