



*The New Private Security Industry:*  
**Regulating  
Cybersecurity  
Services  
in South Africa**



**PSIRA**  
Private Security Industry Regulatory Authority



## About the Report

**Title:** *The New Private Security: Regulating Cybersecurity Services in South Africa*

**Author:** Hloniphani Xulu

**Publisher:** Private Security Industry Regulatory Authority©

**Year Published:** 2022

**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.



**PSiRA**

Private Security Industry Regulatory Authority



## Abbreviations and acronyms

<b>BEC</b>	Business Email Compromise
<b>CCMA</b>	Commission for Conciliation, Mediation and Arbitration
<b>CCTV</b>	Closed Circuit Television
<b>CIPC</b>	Companies and Intellectual Property Commission
<b>CSOC</b>	Cybersecurity Operations Centre
<b>CSSP</b>	Cybersecurity Service Provider
<b>e.g.</b>	for example
<b><i>et al.</i></b>	“and others”
<b>ICAO</b>	International Civil Aviation Organisation
<b>ICASA</b>	Independent Communication Authority of South Africa
<b>IMO</b>	International Maritime Organisation
<b>IP address</b>	Internet Protocol address
<b>ISPA</b>	South Africa’s Internet Service Providers’ Association
<b>ISP</b>	Internet Service Provider
<b>ISSP</b>	Internet Security Service Provider
<b>IT</b>	Information Technology
<b>MOU</b>	Memorandum of Understanding
<b>MSP</b>	Managed Service Provider
<b>MSSP</b>	Managed Security Service Provider
<b>NSFAS</b>	National Student Financial Aid Scheme
<b>PSIR Act</b>	Private Security Regulation Act 56 of 2001
<b>PSiRA</b>	Private Security Industry Regulatory Authority
<b>PSSP</b>	Physical Security Service Provider

---

<b>R&amp;D Unit</b>	Research and Development Unit
<b>SAPS</b>	South African Police Service
<b>SAQA</b>	South African Qualifications Authority
<b>SASSETA</b>	Safety and Security, Sector Education and Training Authority
<b>SITA</b>	State Information Technology Agency
<b>SOC</b>	Security Operations Centre
<b>SOE</b>	State Owned Entity
<b>TVET</b>	Technical, Vocational Education and Training
<b>UK</b>	United Kingdom
<b>US</b>	United States
<b>USB</b>	Universal Serial Bus
<b>VPN</b>	Virtual Private Network

---

# Table of Contents

Abbreviations and acronyms .....	iii
Executive Summary .....	1
1. Introduction.....	2
2. Background of the Study .....	3
3. Research Aim, Objectives, Hypothesis and Questions .....	5
4. Research Methodology .....	6
5. Literature Review .....	7
5.1. The Impact of Revolutions on the Private Security Industry .....	7
5.2. The Crime and Involvement of Private Security Industry.....	10
5.3. The Dynamics of Cybersecurity.....	12
5.4. The Impact of Cybersecurity on Critical Infrastructure .....	14
5.5. The Regulation of the New Private Security Industry.....	15
6. Research Findings.....	17
6.1. The Existence of Cybersecurity Service Providers .....	17
6.2. The Difference between Managed Services and Managed Security Services.....	18
6.3. The Comparison of Physical and Cyber Security Service Providers .....	19
6.4. The Commonly Witnessed Cybercrime.....	21
6.5. Security Measures and Cybersecurity Services used to deal with Cyberattacks.....	25
6.6. The Requirements for Cybersecurity Specialist(s) .....	30
6.7. The Sourcing of Cybersecurity Services .....	31
6.8. The Requirements for a Cybersecurity Company .....	31
6.9. The Certifications and Accreditation of Cybersecurity Training.....	31
7. The PSIR Act and the Regulation of the Cybersecurity Industry .....	38
8. Recommendations .....	40
9. Conclusion .....	41
10. References.....	44





## Executive Summary

The heavy reliance on digital platforms, computer systems and computerised processes of doing things created a need to protect these aspects of people's lives. If indeed by foul means they are interfered with, repercussions stand to be longstanding and disastrous, possibly catastrophic. Many organisations worldwide came up with strategies to safeguard cyberspace. The introduction of cyberspace and criminal activities led to the formation of new security measures and services to prevent those criminal acts. For this reason, there is a new private security industry that has emerged alongside the old private security industry. The new private security is cybersecurity.

This new private security raises the question of whether or not PSiRA has a mandate to regulate the newly emerged industry. Needless to say, there are officers and companies which are involved in protecting organisations and other establishments from various forms of cyberattacks. It is for this reason that PSiRA undertook this study to establish the extent of rendering cybersecurity services in South Africa and to establish the relevant legislation for the regulation of rendering cybersecurity services and its providers. Exploratory in nature, this study used a qualitative research approach to explore, examine and understand the regulation of cybersecurity services and their providers in South Africa.

Cybersecurity services are security services that are rendered in cyberspace, which differ from the traditional security services. The objective and role of cybersecurity service providers and that of physical security service providers remain the same. Both security service providers render different types of security services to another for reward, remuneration, fee or benefit.

The PSIR Act is arguably the applicable legislation to regulate cybersecurity services. Whilst the Act does not specify where the security services could be rendered, security services rendered in cyberspace are security services in a different space. It is for this reason that cybersecurity service providers must be regulated in terms of the PSIR Act.

## 1. Introduction

In his article titled: “The New Private Security Industry, The Policing of Cyberspace and The Regulatory Questions”, Button (2020) made observations that there is a new private security industry that has emerged alongside the old private security industry. Button’s (2020) article generated interest among researchers on this novel industry, and on the need for its regulation. This study lays a foundation for the new private security industry to which Button (2020) refers. There is heavy reliance on digital platforms, computer systems and computerised processes of doing things and this creates a need to protect these aspects of people’s lives. Furthermore, if indeed by foul means these are interfered with, repercussions stand to be longstanding and disastrous, and possibly catastrophic (Nadikuttu, 2020). Hence, many organisations worldwide have come up with strategies to safeguard their cyberspace. The new private security industry is called cybersecurity (Button, 2020).

Scholars provide diverse definitions of cybersecurity. Craigen, Diakun-Thibault and Purse (2014) define cybersecurity as the organisation and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign *de jure* from *de facto* property rights. Lewis (2006) defines cybersecurity as the safeguarding of computer networks and the information they contain from penetration and malicious damage disruption. Cybersecurity is often used interchangeably with the term Information Technology (IT) security (Von Solm and Van Niekerk, 2013). Both terms refer to the protection of systems, networks, programs, devices and data from cyberattacks. Cybersecurity has created new security service providers such as moderators (Button, 2020). He further compared moderators’ activities in cyberspace to those of security guards in the physical world (Button, 2020). In addition, Button maintained that they also share common traits such as low pay, high labour turnover, and having to deal with incidents that lead to a psychological toll on them.

Over and above the gap that was identified about the new private security industry, Button (2020) also pointed out that cybersecurity service providers (CSSPs) such as moderators were not well studied. The question that arises in this instance is whether there is a need to regulate cybersecurity as one of the fields of private security. Section 4(d) of the Private Security Industry Regulation Act 56 of 2001 (PSIR Act) makes provision that the Authority should conduct ongoing studies on the rendering of security services and practices of security service providers to identify shortcomings in the Act and the Levies Act, or any policy or rule made in terms thereof. Hence the importance of this study.

As the world evolves, we continuously witness many changes occurring in a blink of an eye. As the regulator of private security in South Africa, PSiRA must pay more attention to security services that emerge because of cyber-threats, namely cybersecurity services. Cybersecurity, by its very nature, is a broad concept that involves interesting components.

Firstly, this report presents the background of the study. Secondly, it covers the research aim, objectives, hypothesis and questions. Thirdly, it presents the research methodology. Fourthly, it unpacks the literature review. Fifthly, the report presents research findings, and lastly, it makes recommendations and draws a conclusion.

## 2. Background of the Study

The Third Industrial Revolution introduced electronics and information technology to society intending to automate production (Roberts, 2015). It is evident that this industrial revolution did not only bring about technological changes, but it introduced a concept of the internet which can be regarded as another world. Vrana (2012, p. 91) maintained that the internet had become an environment that enables real-time dynamic interaction, facilitating global opportunities such as rapid communication, socialising, information and sharing, banking, the sale and purchase of goods and a vast array of business activities and information services. The existence of the internet has made people's lives easy all over the world. The statistics of the global digital population shows that in January 2021, there were 4.66 billion active internet users worldwide, which constituted 59.5 per cent of the world global population (Johnson, 2021). This means that the internet is utilised in many aspects. The increase in demand of the internet exposes its users to various criminal activities also known as cybercrimes (Dubois & Jreije, 2006, p. 178 and Vrana, 2012, p. 91).

Cybercrime is not a new phenomenon; it has been researched for more or less a decade. Criminologists such as Majid Yar (2005) and Furnell (2003) view cybercrimes as familiar criminal activities pursued with some new tools and techniques. In affirmation of the previous assertions, Button (2020) contends that crime has changed because of where people do things. Furthermore, the transformation of criminal activities such as hacking has been extensively driven by the technological revolution (Button, 2020). The cybercrime phenomena made scholars like Dubois and Jreije (2006, p. 178) and Vrana (2012, p. 91) on their studies to point out that the first line of defence from cybercrimes is usually internet security service providers (ISSPs), well known as cyber or managed security service providers (MSSPs). These scholars argued that MSSPs offer various strategies to secure cyberspace (Dubois & Jreije, 2006, p. 178; and Vrana, 2012, p. 91). Vrana (2012, p. 92) noted that there are different types of services offered by CSSPs, namely antivirus software, intrusion

detection, anti-spam software, firewalls, etc. Studies show that most organisations worldwide appoint the so-called MSSPs. It is submitted that South African organisations are insourcing or outsourcing internet security services to CSSPs.

The establishment, structuring and conduct of security services are outlined in section 199 of the Constitution of the Republic of South Africa (1996). Section 199(1) provides that security services of the Republic consist of a single defence force, a single police service and any intelligence services established in terms of the Constitution. Sub-section (3) further states that other than the security services established in terms of the Constitution, armed organisations or services may be established only in terms of national legislation.

Sub-section 4 proceeds to say, the security services must be structured and regulated by national legislation. Therefore, any other security services that are not listed in section 199 (1) of the Constitution of the Republic are supposed to be regulated by the PSIR Act. Section 1 of the PSIR Act provides definitions of what a security service means. As part of the definitions provided, security service means protecting or safeguarding a person or property in any manner.

Defining cybersecurity services in the context of the PSIR Act is critical. Firstly, a person needs to view cyber (internet) as the space in which security services are rendered. Secondly, one needs to treat systems, networks, programs, devices and data as an individual or organisation's belonging, which brings another element of the definition provided by the Act which is the property. The list can be classified as a property that needs to be safeguarded or protected against cyberattacks. Cybersecurity service means the protection or safeguarding of systems, networks, programs, devices and data in any manner. The officers who are involved in protecting or safeguarding data in cyberspace are referred to as moderators or cybersecurity specialists (Button, 2020).

According to section 1 of the PSIR Act, a security service provider is a person who renders a security service to another for remuneration, fee or benefit and includes such person who is not registered as required in terms of the Act. CSSPs render internet or IT security services to persons or organisations for remuneration, fee and benefit. In short, they exist for profit. The Authority is mandated by law to regulate cybersecurity services that include services rendered by MSSPs and other CSSPs. If the opposite is true, the regulatory questions still stand - who should regulate the new private security industry and empowered by which law?

### 3. Research Aim, Objectives, Hypothesis and Questions

The study aims to unpack cybersecurity and make possible recommendations on how it can be regulated in South Africa.

The objectives of the study are to:

- *Ascertain different security services rendered by CSSPs.*
- *Establish whether the PSIR Act grants PSiRA powers to regulate cybersecurity services and their providers in South Africa.*
- *Establish whether there is a regulator that is currently governing cybersecurity services.*
- *Establish the role of South Africa's Internet Service Providers' Association in regulating and ensuring compliance of cybersecurity service providers.*
- *Discover the security measures used to prevent cyberthreats.*

The research hypothesis of this study is as follows:

*As a security service, cybersecurity is governed by the PSIR Act, which obligates cybersecurity providers to register with the Private Security Industry Regulatory Authority.*

The primary research question is, which law(s) regulate the rendering of cybersecurity services in South Africa?

The secondary research questions are as follows:

- *What is the nature of security services rendered by cybersecurity service providers?*
- *What powers does the PSIR Act grant PSiRA to regulate cybersecurity services and their providers in South Africa (if at all)?*
- *Which regulator is currently regulating the rendering of cybersecurity services?*
- *What is the role of Internet Service Providers Association in regulating and ensuring compliance of cybersecurity service providers?*
- *What security measures are used to prevent cyberthreats?*

## 4. Research Methodology

This section details the procedures and techniques that were used in conducting the research. It is believed that access to the reality of the newly emerged private security industry can be gained through social construction. Hence, the study adopted the interpretivism research paradigm. This philosophical doctrine allows one to view the world through the perceptions and experiences of participants (Thanh & Thanh, 2015, p. 24).

When seeking answers for the study, researchers who follow the interpretivism research paradigm use those experiences to construct and interpret their understanding from the collected data (Thanh & Thanh, 2015, p. 24). The reality, therefore, is socially constructed (Thanh & Thanh, 2015). It is commonly known that interpretivists or constructivists predominantly use qualitative research approach or method because it provides rich reports that are deemed necessary for interpretivists to fully understand contexts. Thus, this report adopted a qualitative research approach to explore, examine and understand the regulation of cybersecurity services and their providers in South Africa. Qualitative research approach uses various instruments to collect data, among others are interviews, observation, etc.

This study utilised interviews with semi-structured questions as a data collection instrument. The reasons for the usage of this instrument were that, firstly, it enabled one to pose clarity seeking questions where necessary, meaning it gave flexibility for one to probe by using follow-up questions where appropriate. Secondly, it reduced the chances of participants not responding to some questions that were asked. Thirdly, unlike a questionnaire, this instrument reduces the likelihood for research participants not to answer the questionnaire in time due to that they have forgotten.

The types of interviews that were used were face-to-face and telephonic. There is another type of interview that has emerged called virtual interviews. Virtual interviews refer to interviews conducted using digital techniques such as Skype, Microsoft Teams and others (Bertrand & Bourdeau, 2010). Where necessary, virtual interviews were used.

In terms of sampling, the study used purposive sampling. Landreneau and Creek (2009) define purposive sampling as the selection of participants based on the characteristics they possess. Therefore, the study selected each participant based on the characteristics they showed and in line with the objectives of the study. The sample of this study consisted of local and international CSSPs, academics, training institutions and other relevant stakeholders.

This study sought to establish a specific mandate, namely whether PSiRA has the mandate to regulate the rendering of cybersecurity services and its providers in the country. The study identified and gave a brief understanding of each sector for further research studies to be conducted. In addressing ethical issues such as anonymity and confidentiality, a consent

form was developed to outline how the participants' information and identities were to be secured. The researcher used content analysis to process collected data. Member checking method was used to confirm the validity and reliability of the findings. According to Harper and Cole (2012, p. 1), member checking refers to the quality control process by which one seeks to improve the accuracy, credibility and validity of what has been recorded during a research interview. This research report was sent to research participants to check whether the findings truly reflect the views, feelings and experiences of the selected interviewed participants.

## **5. Literature Review**

This part discusses the existing literature on cybersecurity.

### **5.1. The Impact of Revolutions on the Private Security Industry**

Numerous revolutions have impacted and continue to impact societies in various ways, the most prominent one being industrial revolutions. In their nature, revolutions are abrupt and bring about radical changes (Schwab, 2017). This literature review did not dwell much on industrial revolutions as the study was not formulated around them. Nevertheless, they assisted in understanding where some security services emanate from, particularly cybersecurity services. In his book, Schwab (2017) affirms that there is a series of industrial revolutions that have occurred, tracing back to the First Industrial Revolution up to the recent one, the Fourth Industrial Revolution. Schwab (2017) maintains that it is important not to overlook the Agrarian Revolution, which occurred 10 000 years ago before the industrial revolutions because somehow it also contributed to some activities that are still witnessed even in this era.

#### **5.1.1. First Industrial Revolution**

The concept "industrial revolution" denotes major industrialisation and innovation that occurred in Great Britain in the late 17th and 18th centuries (Deane, 1979; Mathias, 2013). The industrial revolution, according to Mathias (2013), was characterised by the utilisation of steam-powered engines, the growth of factories and the mass production of manufactured goods and services. It is contended that these observations were made by the British philosopher, Arnold Toynbee (Deane, 1979, p. 2). The philosopher pinpointed all those industrial changes when he was delivering a lecture on the subject matter at the University of Oxford in 1880 (Deane, 1979). Toynbee's view went unchallenged for more than half a century, which then led to his observation being labelled as the First Industrial Revolution (Deane, 1979).

Due to the invention of steam-powered industries for mass production, which was introduced by the First Industrial Revolution, communities began to witness urbanisation

since some industries were built in urbanised areas (Mathias, 2013; De Vries, 2013). Gollin, Jedwab & Vollrath (2016) emphasised that industries needed workforces to be productive, which created a crisis of overpopulation in nearby industries because people, in particular workers, began to settle next to those industries. Moreover, most people were moving towards urban areas to seek economic opportunities and improve their living qualities (Soh, 2012, p. 291). At times, people would move to urban areas and not be fortunate enough to secure those economic opportunities. Thus, Soh (2012) maintained that the rapid urbanisation contributed to other factors and crime was one of them. Furthermore, it is argued that overpopulation created a security challenge for residents, the working class and the police since they had to battle with crime (Soh, 2012).

### **5.1.2. Second Industrial Revolution**

This industrial revolution was characterised by the introduction of many new technologies which amongst others was the invention of electricity, steel production, which led to the creation of trains, railways, oil and petroleum (Atkeson & Kehoe 2001). For example, the invention of trains as a mode of transport exacerbated some of the criminal activities within that sector, which made the railway sector to outsource some security services to the private security industry to fight those criminal activities (Minnaar & Ngoveni, 2004). PSiRA undertook a study conducted by Zama and Caluza (2020) to understand security services rendered in the railway sector and determined how the sector could be regulated. In a nutshell, the Authority is aware of security activities that emanated due to this industrial revolution and made efforts to ensure that they are effectively regulated.

### **5.1.3. Third Industrial Revolution and “Quiet” Revolutions**

The Second Industrial Revolution was then followed by the Digital Revolution, which was comprised of computers and Information Technology used for mass production, communication, etc. This industrial revolution was first referred to as the “Green Industrial Revolution” and later labelled as the Third Industrial Revolution by an American sociologist and economist, Jeremy Rifkin (Janicke & Jacob, 2013). Remember, the First Industrial Revolution introduced the concept of urbanisation – “the increase in the number of cities and urban population is not only a demographic movement but also includes social, economic and psychological changes that constitute the demographic movement” (Srivastava, 2009, p. 75). Then the Third Industrial Revolution came with the concept of globalisation – “the growing interdependence of the world’s economies, culture, and populations brought by cross-border trade in goods and services, technology and flows of investment, people, and information” (Kolb, 2018).

In summarising the above paragraph, Kolb (2018) argued that globalisation resulted in countries building economic partnerships. As it was earlier discussed in the background



of the study, this industrial revolution introduced the internet to society and the internet created a virtual space famously known as cyberspace. Furthermore, it was debated by Vrana (2012, p. 91) that the internet has become an environment that enables real-time dynamic interaction, facilitating global opportunities such as rapid communication, socialising, information and sharing, banking, the sale and purchase of goods and a vast array of business activities and information services. Henceforth, globalisation would have not been fast-tracked the way it is nowadays if the Internet and other digital platforms were not created. Globalisation was mostly fueled by an introduction of electronics and information technology to societies as Vrana (2012) argued.

As countries were starting to trade with one another, Siboni and Sivan-Sevilla (2017) observed that decision-makers began to encounter various challenges brought about by cyberspace. They further emphasised that cyberspace facilitates the flow of information, which in most cases leads to economic prosperity, efficiency and social benefits. They also stressed that cyberspace is a target for national security, criminal and commercial threats (Siboni & Sivan-Sevilla, 2017, p. 83). Hence, societies started to witness new forms of criminal activities, which are caused by the people and organisations' reliance on cyberspace (Siboni & Sivan-Sevilla, 2017). The change of crime contributed to the transformation of policing strategies. This phenomenon is best described by what was termed as a "Quiet Revolution" (Steering & Stenning, 1976; Button, 2020).

Scholars state that there is a Quiet Revolution that is taking place alongside industrial revolutions, and its focus is on the transformation of policing strategies and security services as informed by the change of criminal activities (Steering & Stenning, 1976; Button, 2020). It was first observed by Steering and Stenning in the late 1970s and early 1980s. The first Quiet Revolution was based on the significant changes that were occurring in policing. Button (2020) argued that Steering and Stenning observed the extensive increase of private security associated with the increase of private property and the underfunding of the police, with a sector focused upon preventive rather than curative policing. The two scholars observed how those changes were occurring with little debate or scrutiny from scholars and policy makers (Button, 2020). According to Button (2020, p. 39), "a significant number of researchers have built upon their body of research noting the continued augmentation of private security and other forms of private policing and the need for special regulatory and governance structures."

The regulator of the private security industry in South Africa has been conducting studies on the regulatory aspects of what Button (2020) now refers to as the old private security industry (physical security). The Authority has not as yet conducted any study on the change of security services as informed by the Third Industrial Revolution and/or quiet revolutions. This affirms the assertions made by Button (2020) when arguing that scholars have not

conducted studies aiming at understanding the influence of technological revolution and how it impacts the way in which things are done. Furthermore, Button (2020) believed that the increased dependence on the internet or cyberspace created new forms of crime and security measures to counterattack, which he referred to as the beginning of the Second Quiet Revolution.

The Third Industrial Revolution together with the Second Quiet Revolution, according to Button (2020), led to the formation of the “new” private security industry alongside the old one. From Button’s (2020) view, there were new companies providing security services for profit like any other physical security company. However, the new companies were not focusing on physical security as usual, but their focus was on safeguarding cyberspace (digital world), which was a completely new phenomenon that did not intend to replace physical security companies. He further stated that this was never witnessed before in the private security industry, hence he said it is a “new” private security industry alongside the old one (Button, 2020).

#### **5.1.4. The Silent Fourth Industrial Revolution**

One would wonder why the background of the study did not discuss the Fourth Industrial Revolution (4IR), which was coined by Klaus Schwab in 2016. The motive behind this was that Xu, David and Kim (2018) argued that the Fourth Industrial Revolution is building on the Third Industrial Revolution, which was a digital revolution that has been occurring since the middle of the last century. They stressed that 4IR is characterised by a fusion of technologies that is blurring the lines between physical, digital and biological spheres (Xu *et al.*, 2018). This means that cybersecurity services did not emanate from the 4IR. The recent industrial revolution witnessed the advancement of those security services which commenced in the Third Industrial Revolution. It is for this reason that the literature review focused on the Third Industrial Revolution in understanding the phenomena. Be that as it may, the study does include 4IR technologies that impacted the “new” private security industry.

#### **5.2. The Crime and Involvement of Private Security Industry**

Dubios and Jreije (2006) note that in previous years the usage of networking and the internet was only limited to government and university researches. Nowadays, internet usage is mainstream and is being used in many aspects; for private or commercial purposes (Dubios & Jreije, 2006). This means that people and organisations use the internet in different ways.

Globally, scholars argued that because of the internet attracting more and more users, many insecurities amongst its users have been created (Rowe, Reeves & Gallaher, 2009; Vrana, 2012). Most internet users have been exposed to several security threats that come in the form of cybercrimes, which cost them a multitude of financial losses (Rowe, Reeves & Gallaher, 2009; Vrana, 2012). One of the researchers even went to give the total estimation of 388 Billion US dollars which was lost in the year 2011 due to cybercrimes (Vrana, 2012).

The list of cybersecurity threats that exist is endless as these threats change from now and again. Cybercrimes are not new. There are different definitions provided for the phenomena. Cybercrime is a general term used to describe digital or hi-tech crime because of generalisation for criminal and undesirable or harmful behaviour that is assisted or enabled by networked technology (Dlamini & Mbambo, 2019; Dubios & Jreije, 2006). In South Africa, there are two legislations, Cybercrime Act 19 of 2020 and Electronic Communications and Transaction Act 25 of 2002, that define cybercrimes. Scholarly writings show that internet-related crimes are invented by people with intent to steal, trespass, cause vandalism, prove themselves to be elite hackers, or just for thrill and challenge (Dubios & Jreije, 2006). These are the so-called cybercriminals or cyber-attackers. The work of Siboni and Sivan-Sevilla (2017) reveals that the lack of guardianship in cyberspace enabled cybercriminals to exploit numerous hardware and software weaknesses and to use attack tools that succeeded in the previous attacks. Vrana (2012) argues that the most popular ones include fraud, identity theft, theft of intellectual property rights, etc.

Scholars pointed out that cybercriminals utilise a wide range of techniques to accomplish their mission, which includes spamming, smishing, phishing, viruses, malicious code, hacking, infrastructure attacks (denial of service attacks, compromise of sensitive information, time and resources diverted from other tasks, and misinformation), Internet Domain Name System (DNS), an attack against or using routers, network intrusion, XSS attacks, the distribution and supply of illicit data to commit acts of both criminality and undesirable behaviour (Direnzo, Doward & Roberts, 2015; Vrana, 2012). The security of the people and organisations' property against numerous forms of cybercrimes remained a burning question (Alqahtani, Sarker, Kalim, Hossain, Ikhlaiq & Hossain, 2020). This concern, according to Button (2020) and Rowe, Reeves and Gallaher (2009), spawned a wide range of new companies offering security services in cyberspace which are referred to as ISSPs or CSSPs. It is argued that their core mandate is to provide security services to external stakeholders in exchange for profit (Button, 2020).

### 5.3. The Dynamics of Cybersecurity

Before the existence of CSSPs, the literature revealed that cybersecurity concerns were solely the responsibility of internet service providers until the late 1990s when there were companies who established themselves as ISSPs (Allen, Gabbard, May, Hayes, & Sledge, 2003; Oppliger, 1997). Internet Service Providers (ISPs) and ISSPs are not the same despite other views to the contrary. It is our view that both ISPs and ISSPs are third parties that render different services to different markets for benefit. Saadat and Soltanifar (2014) state that ISPs generally refer to the people or companies that provide network and Information Technology (IT) support, wired and wireless telecommunications services required for internet access. Briefly, ISPs are internet access providers regulated by the Independent Communication Authority of South Africa (ICASA).

ISSPs refer to people or companies that protect internet users from cyber-related crimes using different types of managed security services (Ding, Yurcik & Yin, 2005). In short, their main aim is to provide security services and as the researcher observes, they are not regulated by any regulatory authority including ICASA because they are rendering security services in cyberspace. PSiRA has a mandate to regulate security service providers as provided in section 3 of the PSIR Act. This study excluded ISPs that exclusively provide 'managed services'. It is noteworthy to consider the argument advanced by Rowe *et al.* (2009) and Vrana (2012) that some ISPs are still offering different types of cybersecurity services to their clients. Therefore, ISPs that provide both services to their clients do form part of this study. Ding *et al.* (2005) assert that CSSPs render different security services to their clients. The following table formulated by Ding *et al.* (2005, p. 12) shows different types of cybersecurity services that are provided by MSSPs.

SERVICES	DESCRIPTION
Application security/code review	Scan web application code for vulnerabilities and insecure coding techniques.
Security policy compliance.	Perform regularly scheduled audits to ensure continued compliance and identify nonconformance with a company's established information security policy and government or industry-specific regulations (e.g. Sarbanes-Oxley and HIPAA).
Vuln. assessment and management	Perform penetration test on systems for known vulnerabilities.
Certificates	Assessing firms' compliance with government, industry, partner and customer requirements, and issuing proof of compliance.

SERVICES	DESCRIPTION
Risk management	Help customers to make decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost-effective controls.
Managed firewall services	24/7 monitoring of all traffic through a firewall for service outage.
Managed VPN services	Similar to managed firewall services, usually a firewall is an add-on.
Email anti-spam/antivirus	Scan content (email messages and attachments, SMTP, HTTP, FTP, file transfers) for potentially malicious code or junk mails.
Managed IDS	24/7 monitoring of all network traffic, detecting and analysing anomalies for true attacks.
Security monitoring	Similar to IDS, can draw data from a wider variety of sources and provide more in-depth analysis.
Threat intelligence	Based on the provider's research on real-world events, offers a series of features including early warning of emerging threats, threat severity measurement, immediate notification and consultation.
Incident response and forensics	Respond to security breaches based on five cornerstones of effective incidence management and response: detection, assessment, forensics, containment and recovery.
Authentication	Verifies and confirms the identity of individuals who are accessing sensitive information, or conducting high value B2B transactions on an extranet.
Identity management	Administers user authentication, access rights, access restrictions, account profiles, passwords and other similar attributes.
Consulting	The practice of helping firms to improve security levels through professional analysis.

Ding *et al.* (2005) assert that the list of managed security services keeps on expanding as the demand for new security technology emerges. The table above also reveals some concepts or security services that the private security industry is familiar with, such as consultancy, intruder detection, etc. Section 1 of the PSIR Act makes provision about the people who

give advice on the protection or safeguarding of a person or property, on any other type of security services.

Abu-Taieh (2017) asserts that firewalls control access from network to network, meaning they prevent access between networks. However, it is argued that they cannot provide a signal in case of an attack (Abu-Taieh, 2017). Thus, MSSPs decided to develop intrusion detection software. The Act is clear on the devices used for intrusion detection that they are security equipment. Therefore, all intrusion detection software used to prevent cyberattacks form part of this study because their assistance in locating, deciding and controlling unauthorised system behaviour such as unauthorised access, or modification and destruction can be regarded as security equipment.

#### **5.4. The Impact of Cybersecurity on Critical Infrastructure**

According to Drenzo *et al.* (2015, p. 1), “computer networks control some of the most important critical infrastructures in the world”. They refer to examples of critical infrastructures, namely power systems, water supply systems, air traffic control, building control systems, and transportation systems (Drenzo *et al.*, 2015, p. 1). In South Africa, when one refers to “critical infrastructure” they are referring to any infrastructure established in terms of section 16 of the Critical Infrastructure Protection Act 8 of 2019. Past research has shown that the increased interconnectivity of systems and reliance on technology by most critical infrastructures expose them to failures of computer systems and/or deliberate cyber-attacks (Drenzo *et al.*, 2015; Pang, n.d.). Scholars argued that the most highly impacted critical infrastructures are the aviation and maritime sectors (Drenzo *et al.*, 2015; Fox, 2016). Both sectors highly depend on the Global Position System (GPS) for navigation (Drenzo *et al.*, 2015; Fox, 2016). Hence, Drenzo *et al.* (2015) argue that these can be spoofed (deliberate introduction of a false signal) anytime by cybercriminals if not protected. It is for this reason that many organisations appoint CSSPs to protect their computer networks against cyberattacks.

The International Civil Aviation Organisation (ICAO) and International Maritime Organisation (IMO) have played a role in developing security measures and actions to counter any form of criminal acts in that space, which amongst others include cyber-attacks (Fox, 2016). Maritime cybersecurity denotes actions taken to safeguard computer networks and assets both on vessels, ports, terminals, and all electronic hardware supporting sea activities (Pang, n.d.). Aviation cybersecurity means the protection of a wide computer-based interconnected systems, spanning from air navigation systems, onboard aircraft control and communication systems, airport ground systems, flight information systems, security screening, and many other systems used on daily operations of the aviation industry against cyberattacks (ICAO, 2021). ICAO and IMO recommend to their member States to develop a cybersecurity plan.

The involvement of the private security industry in critical infrastructures such as aviation and maritime is not something new. Earlier PSiRA studies have focused on the regulation of security services rendered in the aviation and maritime space respectively. Seanego and Xulu (2020) indicated that while some airports are classified as critical infrastructures, others were not. Zama (2020) further affirmed that some ports are deemed as critical infrastructures. Both studies on aviation and maritime security that were conducted by PSiRA focused on the regulation of physical security and not cybersecurity in the aviation and maritime sector. Hence, *Direngo et al.* (2015, p. 4) recommended that regulators should update regulations and policies from an exclusive emphasis on the 'physical aspect' of security to the 'cyber aspect'. It is accepted that there are possibilities of other critical infrastructures being affected by cyberattacks. However, they might not have received attention as we see in aviation and maritime academic discourse.

### 5.5. The Regulation of the New Private Security Industry

Organisations prefer to outsource cybersecurity services to MSSPs because they are more cost-effective than appointing in-house cybersecurity officers (*Ding et al.*, 2005). One of the contributing factors for outsourcing cybersecurity services is the ongoing evolution of cyberattacks which requires them to provide refresher training to their cybersecurity officers every time, and the training is expensive (*Ding et al.*, 2005; *Pedley, Borges, Bollen, Shah, Donaldson, Furnell & Crozier*, 2020). Moreover, *Ding et al.*, (2005) asserted that MSSPs have more experience, updated technology, better-trained expertise and serve diverse clients. The challenge that emerging MSSPs may face is that organisations that contract MSSPs will prefer those with more clients than emerging ones (*Ding et al.*, 2005). These firms hold a view that having more clients also contribute to the improvement of service quality. A service provider that monitors more networks is more likely to correlate attacks, identify new attacking patterns and warn customers of events beyond their perimeters (*Ding et al.*, 2005). Clients, therefore, indirectly contribute to the monopolisation of the industry.

*Button* (2020) states that cybersecurity introduced new roles such as the role of moderators. He compared their activities in cyberspace to those of security guards in the physical world (*Button*, 2020). He also maintained that they also share common traits such as low pay, high labour turnover, and having to deal with incidents that lead to a psychological toll on them (*Button*, 2020). Section 4(m) of the PSIR Act provides that the Authority must promote the protection and enforcement of the rights of security officers and other employees in the private security industry. By extension, CSSPs' rights must be protected by the PSIR Act. *Button* (2020) avers that some roles created by the newly emerged private security industry, such as testers or ethical hackers, have been occupied by the past criminal hackers because of their proven skills.

Many studies have been conducted by scholars worldwide on the regulation of the activities that occur in cyberspace. However, no research publications focus on the regulation of rendering “private” cybersecurity services and their providers. Button (2020) does not address the question of who should regulate the rendering of cybersecurity services and their providers, hence the importance of this study. It is submitted that if CSSPs are not effectively regulated, companies may be hesitant in outsourcing their network security to MSSPs and other CSSPs (Ding *et al.*, 2005, p. 1).

Ever since the inception of the Digital Revolution, the regulation of security services was more on the physical technology which was introduced by this industrial revolution, leaving cybersecurity generally unregulated. This opened a wide gap in the regulation of the private security industry. While PSiRA is mindful of the existence of CSSPs, it is not well versed with the particular security services rendered. The question of who should regulate the rendering of those services remains a moot question. Despite cybersecurity training being relatively expensive, section 3(j) of the PSIR Act mandates PSiRA to promote high standards in the training of security service providers and prospective service providers. Currently, the Authority does not accredit cybersecurity training institutions.



## 6. Research Findings

This part presents the analysis and interpretation of the data collected in this study. In doing so, it provides answers to the research questions detailed in the research methodology.

### 6.1. The Existence of Cybersecurity Service Providers

The drivers behind the existence of CSSPs in South Africa differ from one company to the other. The common denominator for such existence is the obvious existence of cyberspace and criminal activities created by the 'lack of guardianship' within that space. There was a golden opportunity to make money while protecting and safeguarding that space for others. It may be argued that during the formation of CSSPs, the objective was to be proactive or reactive towards cybercrime. The reality is that their formation was associated with profit maximisation and 'lack of guardianship' within the country's cyberspace. CSSPs, therefore, had to protect and safeguard the people and organisations' properties in the digital world or cyberspace.

#### 6.1.1. The Impact of Cybercrime in the Public and Private Sector

The weaknesses of State Information Technology Agency (SITA) networks allowed criminals to exploit the government Information Technology (IT) systems. The government witnessed an evolution of financial fraud within its institutions, which necessitated different measures to be put in place to prevent such criminal acts. It was gathered that the government was losing a lot of money because of the criminal syndicates who were creating ghost employees and contractors and stealing data to sell it to outsiders. After realising that the type of financial fraud which they were exposed to was not because of a physical security breach but a cybersecurity breach, the government decided to call upon experts in the field of cybersecurity to protect their cyberspace against various forms of cybercrime. Some of these experts started to form companies to provide cybersecurity services.

The concern of cybercrime was both in the public and private sectors. As aforementioned, the reasons for their existence may be proactive or reactive. Some companies stated that when they started offering cybersecurity services, their focus was more on the reactive approach to cyber incidents than being preventative. As time went by, they began to promote a proactive approach to cybercrime. They invited the public and private sectors to get on board in limiting opportunities for cybercrime to take place. The private sector had more opportunities for CSSPs to source clients than the public sector. This is one of the reasons why there are many companies offering cybersecurity services in the private sector than in the public sector.

### 6.1.2. Internet Service Providers Migrating to Cybersecurity

There are ISPs whose primary objective is to provide internet access to the people and organisations who end up putting cybersecurity services or internet security services as a value-added service to their clients. Other ISPs completely migrated to cybersecurity. The reason behind is none other than profit maximisation and taking advantage of ‘the lack of guardianship’ within cyberspace. It was stressed that clients would appreciate the work of ISPs in providing them with access to the internet. After accessing the internet, the client would seek advice from the ISP on how to secure their network. Due to the ISP’s drive for profit maximisation, they never say they do not provide cybersecurity services. They sometimes inform their clients that they also provide cybersecurity services, which is incorrect. If the client gives them the job, they would subcontract this service to a company with such expertise. These companies would advertise for cybersecurity services and subcontract once contracted. This is how some ISPs are contracted to ‘offer’ cybersecurity services. There are a lot of ISPs in the country that provide cybersecurity services, however, one needs to take into consideration the fact that their primary function is not to protect but it is to provide access to the internet.

### 6.2. The Difference between Managed Services and Managed Security Services

Before providing the distinction between managed services and managed security services, it is noteworthy to contextualise the concept of “managed” as used in this study. According to the Oxford dictionary, to manage means to run or control. In the IT domain, ‘managed’ means running or taking control of services (be it IT services or cybersecurity services) on behalf of the client in return for profit. These services can either be insourced or outsourced. In many instances, clients prefer to outsource these services to a third party. The client may wish to outsource due to their incapacity to insource these services. The client and prospective service provider would get into a contractual agreement.

It is difficult to determine the difference between managed services and managed security services. This is simply because cybersecurity or IT security services cannot be separated from IT services. Managed services and managed security services may look the same, but they are not necessarily the same as they have different objectives altogether. When one refers to a managed service, it is about IT support services that are remotely run by a third party. One of the participants stated that “managed service means your technology sits with me and I support it for you.”

If a client requires assistance with any IT services, they would approach a company that offers or specialises in those services and pay them to manage their IT services. In a nutshell,

a company that provides managed services manages any type of IT services for a client. For example, the company would manage emails, networks, cloud storage, systems, software, hardware, etc.

Managed security services refer to the protection of the clients' IT services against any form of cybercrime (be it physical or digital). It is commonly known as IT security and is also referred to as cybersecurity. This means MSSPs provide "certain" cybersecurity services on behalf of the client. The rationale behind the use of the word "certain" is that not all cybersecurity services can be provided as managed security services. There are specific cybersecurity services that can be provided as a managed security service. To mention but a few, a client may purchase firewalls, intrusion detection systems and anti-viruses then MSSPs would manage all those security software for a client in their security operations centre (SOC), also referred to as cybersecurity operations centre (CSOC). SOC or CSOC refers to a room with screens where a cybersecurity officer monitors for suspicious activities in the cyberspace of their client. SOC looks almost like a control room where firewalls and other anti-malware software are monitored. One could compare MSSPs to outsourced security service providers. MSSPs get into long-term contracts with their clients for services rendered just like security companies that protect office parks, retails, residential estates, etc.

There are also cybersecurity services that cannot be sold as managed security services such as forensic investigation, penetration testing (including ethical hacking services), consultancy services, etc. However, the demand for managed security services is too high and this leads to most CSSPs who advertise consultancy services to also provide managed security services. The motive behind this is to secure the contract. By their nature, consultancy services are not necessarily linked to managed security services but are simply advisory services offered separately. The discussion on managed security services is beyond the scope of this study.

The argument by Rowe *et al.* (2009) and Vrana (2012) that some MSPs do provide managed security services to their clients is indeed correct. This study found that no sanction prohibits companies from offering both services, hence there are MSPs and MSSPs which provide both managed services and managed security services to their clients. These provide IT support services as well as cybersecurity services.

### **6.3. The Comparison of Physical and Cyber Security Service Providers**

Physical security service providers (PSSPs) refer to security service providers that are defined in section 1 of the PSiR Act and which are currently regulated by the PSiRA. The idea of protecting property in the physical and cyber spaces from any criminal activities is the same.

However, the practical realities in these spaces are completely different. Therefore, PSSPs and CSSPs operate in different worlds, one being in the physical realm and the other in the digital world also known as cyberspace. The services rendered by PSSPs and CSSPs to their clients include protecting clients or their properties; investigating criminal activities; advising clients on security measures to be implemented in the protection of the property and/or persons; responding or reacting to security breaches; distributing or selling security equipment; training candidates to be security specialists; monitoring signals or transmissions from security equipment; managing, controlling, and supervising the rendering of security services. These service providers render their services in the physical and cyber spaces for remuneration, reward, fee or benefit.

As aforementioned, there is a huge difference between the PSSPs and CSSPs. Their geographical locations are not the same. PSSPs are quite limited to their geographical space, which is within the physical environment. Criminal activities targeting this space are confined within the South African borders. Crimes committed in the physical space are committed locally, which is why there are a lot of geographical restrictions for PSSPs. The interconnectivity brought by the internet to people has exposed them to global threats, otherwise known as cyberthreats. For this reason, geographical restrictions for CSSPs are less than those of PSSPs. Crimes that CSSPs deal with could emanate from anywhere in the world, local or international. It is important to note that the two service providers are not competitors in the provision of security services. The needs of PSSPs and CSSPs clients are not the same, as these provide different services. By its nature, property in cyberspace is mostly intangible. However, a few elements are tangible. Within the physical space, the property is tangible and includes buildings, vehicles and other valuable assets.

Cybersecurity services are more technology-driven than inclined to physical contact. In the physical realm, human beings (security officers) are the ones who patrol premises. In some instances, they carry and make use of firearms. This is not the case in the protection of property in cyberspace. In cybersecurity, they use software and programs designed to quell threats. In this case, suspicious activities are managed using technology. CSSPs, therefore, provide security services in a different space. Anything that has to do with software, networks, servers and computers relate to IT services whereas cybersecurity services are IT security services.

Sometimes cybersecurity awareness training offered to clients minimises the chances of being hacked or exposed to other forms of cybercrime. It was pointed out that cybercriminals sit behind a computer and create phishing links that are used to attack computers. This form of crime does not require the criminal to be in possession of a firearm to attack. CSSPs offer awareness training as a security service, which is not common in the physical security environment.

While PSSPs use tangible security equipment, such as alarms and cameras, CSSPs use intangible security measures, such as anti-virus and anti-malware. Some CSSPs are product vendors. Product vendors sell and install a lot of technology used in the safeguarding of cyberspace. Clients and MSSPs purchase different software and programs from those product vendors to prevent cybercrime. The software does access control and intrusion detection. In physical security, it is the human being who does that with the assistance of tangible security equipment such as alarms. The role played by human beings in cyberspace is to monitor signals coming from the deployed technology. In the physical space, in the event of a break-in by an intruder (into a building), PSSPs could track where the intruder gained entry. This is different with regards to cybercrime and cybercriminals in that a cybercriminal can gain entry into a computer system without a trace. The criminal activity, in this case, will only be picked up once the 'intruder' does malicious activities which will, in turn, trigger the deployed technology.

PSSPs and CSSPs have different expertise, which varies respectively. For this reason, they think and work differently, hence the hiring requirements for CSSPs and PSSPs also differ. While CSSPs possess internationally recognised qualifications, PSSPs possess locally recognised qualifications, such as PSiRA grades and SASSETA training. It is important to also note that while PSSPs are regulated by the PSiRA, CSSPs are not. Whilst CSSPs are not registered by a regulatory body, PSSPs are registered with PSiRA, which is a legal requirement for their operation.

CSSPs can work remotely as they do not have to operate at the client's premises. They can operate from anywhere in the world and provide effective protection to a South African based client. This is impossible with PSSPs because their physical presence at the clients' premises is required (in the case of protecting physical property).

#### **6.4. The Commonly Witnessed Cybercrime**

The existence of cyberspace and virtual communities introduced many activities, one of which is criminal activities. The existence of crime in cyberspace came because of the existence of criminal opportunities resulting from the absence of guardianship. This phenomenon can be best described by the theory coined by Cohen and Felson (1979) known as the Routine Activity Theory. This theory states that crime occurs when a potential offender meets with a suitable target in a place and time lacking guardianship. Linking Routine Activity Theory to the phenomenon subject to this study, it may be argued that cybercriminals use the opportunity to commit cybercrime since they may have observed that there is a lack of guardianship. The growth of cybercrime has resulted in the development of numerous security measures aimed at protecting clients against cyber threats.

Cybersecurity services must be understood within the context of cybercrime. Put differently, to understand what security measures and services are put in place to create guardianship in that cyberspace, it is important to understand the commonly witnessed cyberattacks, bearing in mind that cybercrime can emanate anywhere in the world. The cybercrimes discussed in this part are not only limited to South Africa but are also found internationally. It was revealed that the statistics that were released by the United States (US) secret service show that, globally, organisations are losing \$300 million per month on cybercrimes. It was discovered that many establishments do not publicly disclose the types of cybercrimes committed against them. For instance, there is a well-known Transnet incident which was making rounds in the media that the state-owned entity was allegedly attacked but to date, Transnet has never shared any information on this cyberattack.

As aforementioned, critical infrastructures are targeted by cybercriminals. However, the ones that receive more academic attention are in the aviation and maritime sector. For instance, in South Africa, the railway sector has been a victim of a cyberattack. It is a matter of national security since cybercriminals have targeted a critical infrastructure (Mchunu 2021).

#### a) **Ransomware and/or Malware**

The commonly witnessed cyberattack in South Africa is the use of ransomware, which is a type of malware. The term “malware” is derived from malicious software, which refers to software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system (Mazzotta, 2018). This presents a shift of intrusion that no one thinks of. In cyberspace, intruders use software to gain unlawful entry into somebody’s property. As already mentioned above, physical presence is not a requirement. Examples of malware include computer viruses, ransomware, spyware, worms, trojan horses and other malicious programs.

Ransomware refers to malicious software designed to block access to a computer system until a sum of money is paid (Mohurle & Patil, 2017). In this case, the intruder deploys a virus into a computer intending to encrypt all the files and thereafter demands a ransom to decrypt encrypted files. Encryption means coding information in a way that would not be accessible to any media and decryption is the opposite of encryption. The only way to get the decryption keys is by paying the demanded ransom. This can be frustrating to the hacked computer user as the computer storage would be turned to zero bytes in less than a minute.

Malware can be deployed in different ways, and it is not always deployed through phishing. For instance, a USB containing malware may be physically inserted into a person’s or an organisation’s computer. The deployed malware would start spreading viruses into the

system and/or capturing information then send it back to the alleged criminal. The alleged cybercriminal would then decide what they will do with that information. While others request a ransom, some delete the information in the computer for whatever reason. In preventing cyberattacks, clients will deploy (or cause to be deployed) both physical and digital security measures. Even though the arrangement of cybercrime is intangible, however, certain areas are tangible, which still require physical protection.

## **b) Phishing**

By its very nature, phishing is not an attack, but a mechanism used to deliver an attack. The consequences of phishing would be something like launching malware. Phishing is one of the social engineering techniques used by hackers to obtain information, data or access from a victim. There are many types of social engineering techniques that attackers use to obtain information, data or access. For example, this would include phishing, whaling, vishing, smishing, pretexting and baiting. Phishing can be compared to 'tailgating' in physical security. Tailgating is not burglary or theft, but a technique used by criminals to gain unauthorised access into a property. After gaining access, the commission of crime occurs. Through phishing, a cybercriminal sends a fraudulent email claiming to be from a trusted source. The email may, for instance, claim to be from the bank of the victim and request for the victim's full name, birth date, account number and pin or OTP code. In this case, the intention would be to steal information and/or to access a bank account. A link may also be sent to people working within an establishment and if by mistake an employee clicks the link, this would enable the cybercriminal to gain access. The attack would, therefore, come after gaining access. The only way to stop social engineering techniques is through awareness training programmes. It is for this reason that most establishments offer ongoing cybersecurity awareness training programmes to their employees. Educating employees about social engineering techniques, specifically phishing, remains critical.

## **c) Bots/Botnets**

According to Rowe *et al.* (2009), cybercriminals make use of bots or botnets in conducting their illicit activities. Bots and botnets are compromised computers, which are usually owned by home internet users and small businesses who are unaware that their computers (IP addresses) have been 'recruited' for illicit activities (Rowe *et al.*, 2009). Bots are not only limited to computers but also include any hackable device. This device needs to have an IP address and internet to qualify to be a bot and includes a cell phone, watch, smart TV, CCTV camera and computer. All these devices can be bots or botnets. A bot refers to any device that is infected with malware and is controlled by a cybercriminal to attack others without the owner's knowledge. Devices that are not infected by malware are not bots. Bots are, therefore, compromised hosts just like 'hijacked vehicles'. Bots are referred to as such once they are infected. The concept of botnet arises when there is a network of devices

infected with malware and controlled as a group without the owner's knowledge. A botnet, therefore, refers to a collection of bots. One participant gave an illustration of vehicles hijacked and used to block the highway and these would comprise a botnet.

Sometimes one infected computer cannot successfully attack another computer. When botnets (in the form of more than one computer) are deployed, one computer can be automatically attacked. The *modus operandi* of bots and botnets cannot be confirmed because they change now and again.

Once botnets penetrate a computer system, the command and control of that botnet would have an eagle's eye view on the operations within an establishment. The cybercriminal will be able to determine the establishment's cybersecurity strengths and weaknesses. In this way, it will be easy to launch an attack. Botnets can lay dormant within the establishment's cyberspace for months and years without being identified. If a driver of those botnets sees a need to attack, they would just press a button to activate an attack. Bots are dangerous because many establishments may be victims of bots yet not be aware of their existence.

#### d) **Business Email Compromise**

Business Email Compromise (BEC) is another form of cyberattack that affects most companies in South Africa. BEC is when a cybercriminal gains access to critical information about an organisation or extract money through email-based fraud. They may send an email that seems authentic to a finance department that it must pay a certain amount to a specific account number. The email would appear as if it was sent by a person who occupies an executive or managerial position within a company or organisation. Cybercriminals are capable of intercepting communication between people and redirecting payment to a fraudulent account number. They can even take control of all emails within an organisation.

##### **6.4.1. The Motive behind Cyberattacks**

The motive behind cybercrime varies from one individual and/or group to another. Most cybercrimes are economically and politically motivated. Politically motivated cybercrimes are not on the high end in South Africa as compared to First World countries. Some people are just mischievous in testing their skills by hacking computers. Dubios and Jreije (2006) observed that some internet-related crimes were invented by unscrupulous individuals with the intent to steal, trespass, cause vandalism, "prove themselves to be elite hackers", or just for thrill and challenge. These characters do this just for the fun of it without expecting anything in return.



Other individuals commit cybercrimes because of bitterness, desperation and anger. The anger may stem from being dismissed from an organisation. They may commit cybercrimes with the aid of a cybercriminal. An employee may also steal data from the organisation to defraud it. Sometimes an employee may steal data to sell it.

## **6.5. Security Measures and Cybersecurity Services used to deal with Cyberattacks**

The previous part presented cyberattacks that are commonly witnessed locally and globally. Unlike crime that occurs in the physical realm, which requires a criminal to be physically present when committing the crime, it was observed that the *modus operandi* of cybercriminals cannot be compared to those of ordinary criminals that are found in the physical world. Security measures and services employed to deal with criminal acts arising from the physical and cyberspaces are not the same.

As already mentioned, criminals identified a loophole that security measures used by people and organisations were protecting the physical space and thus leaving the digital space vulnerable. The lack of guardianship within the cyberspace resulted in cybercriminals committing crimes in cyberspace. In dealing with cybersecurity, many establishments are now adopting new security measures and strategies which are completely different from those of physical security.

Button (2020) argued that cybersecurity is a new private security industry and not a continuation of the previous security industry. Button maintained that cybersecurity is a new private security industry because most security measures used to safeguard cyberspace never existed before within the industry. Moreover, companies that provide cybersecurity services did not evolve from the existing industry and they are completely new.

### **a) Firewalls and Intrusion Detection Systems**

Firewalls and intrusion detection systems are regularly used to deal with certain cyberattacks. A firewall strictly deals with cyberattacks that emanate from the internet. A firewall is a software used to control access into a computer network or system. Previously, there was a view that firewalls were not able to inspect and detect computer systems when access was gained because they could not inspect and detect suspicious acts. Firewalls were only designed to control access. Software developers advanced firewalls by incorporating an intelligence layer on top of a firewall, which enables it to be able to detect when access is gained by an unauthorised device and then send a signal to a person who is safeguarding computer networks or systems. Due to this evolution, firewalls can inspect and determine whether there is an attack or not. Cybercriminals use malicious software to gain access to the digital property. To counter this, cybersecurity specialists have come up with firewalls to prevent such attacks.

In a physical security environment, there is a human being (security officer) who performs duties that are like those performed by firewalls in a cybersecurity environment. For instance, a security guard manned at the gate of a property (residential estate or office park) controls access. In a cybersecurity space, those duties are performed by a firewall, which operates as a 'security officer' in cyberspace. The firewall will check who enters a system or when the internet is accessed. It will check the website being opened and determine whether it is suspicious. If it is safe, it will go through. The same happens in physical security, the security officer would check whether the person about to enter the property is not suspicious. Once cleared, that person would be allowed to enter the building. Manning a security guard at the gate does not mean crime will not happen. This is just a measure that is put in place to reduce the chances of crime being committed. The same applies to firewalls. It does not mean that if firewalls have been deployed, then cybercrime will not occur. For instance, if an employee is working outside his or her office, firewalls are unable to detect attacks.

Some CSSPs manufacture or develop, sell, install and distribute anti-malware software such as firewalls and other intrusion detection software. After purchasing anti-malware software, most organisations would appoint a CSSP to manage them on their behalf. This is where managed security services come from. An MSSP may provide various forms of security services which include, but are not limited to, managed threat detection, managed firewall services, managed email security, managed VPN services, managed intrusion detection system and managed intrusion prevention system. Most of these services are rendered in a room staffed by cybersecurity officers who monitor signals from anti-malware software. In the event of a cybercriminal attempting to break into the system, they respond by 'kicking' the criminal out of the system. Where they are unable to detect intrusion and a crime occurs, a defence forensic incident response will be triggered and the investigation will ensue.

## **b) Antiviruses**

Firewalls can only detect cyberattacks that come via the internet. It must be noted that malware cannot only be deployed through social engineering techniques. Sometimes they can be physically deployed through a USB. A cybercriminal may insert a USB containing malware and those viruses would start spreading into that system. Firewalls and intrusion detection software were not designed to prevent malware deployed manually through a USB or other means. Hence, cybersecurity specialists developed antiviruses to deal with malware that enters the computer system manually. An anti-virus would check for infected files and remove them before they disrupt, damage or corrupt a system. Anti-malware and anti-viruses are used as a proactive approach to cybercrime.

### c) Penetration Testing and Ethical Hacking

Penetration testing and ethical hacking are mechanisms used to assess the effectiveness of security measures put in place to protect the organisation's cyberspace. Penetration testing and ethical hacking are separate services. While some cybersecurity companies provide both services, others do not. These mechanisms present a new phenomenon that has never been witnessed in the history of the private security industry. Even if there were mechanisms that certain security service providers used to assess the effectiveness of security measures put in place in the protection of the physical space, they were not offered as a service to another for remuneration, reward or benefit. Needless to say, in the cybersecurity space, security measures are being checked to ensure their effectiveness. These are indeed new security services that came with the new private security industry as argued by Button (2020).

Penetration testing and ethical hacking serve the common purpose of assessing the effectiveness of security measures put in place. While penetration testing assesses intrusions that may enter through a network, ethical hacking checks software strengths, such as anti-malware and anti-virus software. When an establishment intends to undertake a cybersecurity vulnerability assessment, it would appoint a cybersecurity company that renders penetration testing and/or ethical hacking services to conduct intrusion testing by attacking them to determine whether it succeeds. If it succeeds, it will compile a report and present it to the client, presenting all system weaknesses that need to be fixed to prevent future attacks from occurring. The report also contains recommendations of what measures are needed to strengthen their security. Those who install security measures cannot do vulnerability tests of security measures that were installed by them. The vulnerability assessment is done by a third party to avoid a conflict of interest. Hence, some CSSPs solely offer pen tests and/or ethical hacking to another for remuneration, reward or benefit. The two services can either be done at the beginning to check what measures are needed to protect the organisation's cyberspace or at the end to check the vulnerability of security measures that are put in place and thereafter make a recommendation to the client.

There are standard terms used by cybersecurity companies in conducting a pen test. For instance, there is a reference to a *blue team* versus a *red team*. The red team are CSSPs who operate like cybercriminals. They break into an organisation system intending to assist the client to improve the security of their cyberspace. The blue team refers to CSSPs who defend an organisation by putting measures to secure their client's cyberspace. These are installers of security measures. In this way the, 'red vs. blue team' means 'attacker vs. defender'. Generally, penetration testing is conducted by the red team. Pen tests have some

element of physical security within, where the malware is physically deployed through a USB. A pen test also assesses whether there are possibilities for people to enter the building and insert a USB or vandalise servers without being caught.

Ethical hackers are not motivated by or involved in any malicious activities (such as the black hat hackers). Ethical hackers are the so-called 'white hat hackers' who conduct a vulnerability assessment on behalf of their clients. In South Africa, there is a shortage of ethical hackers as the number of existing senior ethical hackers is reported to be no more than 30. It was further reported by the industry that some ethical hackers are not ethical at all, and this presents a regulatory challenge.

One of the regulatory concerns that CSSPs raised is that a person or an organisation that intends to appoint penetration testers or ethical hackers would not know whether they are competent to undertake the work. It was stressed that since there is no regulatory body that certifies South African ethical hackers and pen testers, this poses a serious challenge. It is, therefore, possible that work could be undertaken by incompetent ethical hackers due to the absence of a regulatory body. It was also noted that ethical hacking services are technically illegal because of the absence of legislation. Moreover, the prices for ethical hacking services and pen tests are not fixed.

#### **d) Consultancy Services**

As in the case of physical security where clients seek advice on how they can protect or safeguard their properties, the same is true with cybersecurity. CSSPs advise clients on what security measures should be put in place for purposes of protecting their cyberspace.

#### **e) Private Investigation in the Cyberspace**

From a criminology point of view, when a crime has occurred, an investigation is conducted to systematically search for the truth about how it occurred and who was involved. With cybercrime, there are investigations conducted to discover the truth about cybercrime and the people involved. Investigations are aftereffects, they can either be conducted by public or private security service providers.

In cyberspace, the police are not proactive in the prevention of cybercrime. Instead, they are reactive. It was pointed out that the only time the South African Police Service (SAPS) investigates a cybercrime case is when it is high-profile. If an ordinary citizen is attacked, the police just open a case, which does not arguably receive that much attention from the cybercrime unit of SAPS.

It was also stated that SAPS hardly send their technical experts to small companies for investigations relating to cybercrimes. This has resulted in the growth of private cybercrime

investigators. Most clients prefer to appoint their own private cybercrime investigators to investigate when their cyberspace is attacked. An appointed service provider would compile an evidence pack and generate timelines. They will also share this information with the police. Private cybercrime investigators trace the origins of an attack including the IP address. They also verify whether an IP address used in the attack is linked to the cybercrime suspect. A subpoena for obtaining the equipment of a suspect may be issued and possibly used as evidence in a court of law. The client and service provider will take the police through all the evidence pack before it is presented to the court.

Section 25 of the Cybercrime Act 19 of 2020 provides for powers to investigate, search, access or seize, to any person who is fit and proper. This person should not be a member of the SAPS. One of the regulatory questions that arise relates to the criteria used to identify a cybercrime investigator. The other question relates to the question of which regulatory body determines an individual's status of being "fit and proper". Currently, there is arguably no legislation that supports the establishment of CSSPs in general and cybercrime investigators. It was highlighted that what is deemed as a subject matter expert is seen as an investigator because that person who is deemed as a subject matter expert would have to have the relevant computer forensics qualifications.

Section 25 of the Cybercrime Act provides that any person can be an investigator of cybercrime. This provision presents a controversy in that no requirement is prescribed for one to be an investigator of cybercrime. The Act does not reference a specific law that permits and regulates an identified individual to be an investigator. In the country, an investigator can either be public or private. Public investigators are those who work for the State whereas private refers to persons who in their private capacity offer those services for reward, remuneration, fee, or benefit and are regulated by national legislation as section 199(3) of the Constitution of the Republic stipulates. Section 199(3) categorically states that,

*"Other than the security services established in terms of the constitution, armed organisations or services may be established only in terms of national legislation."*

Therefore, any person who renders investigation services in his or her private capacity must be regulated by national legislation, which in this case is PSiRA. If no legislation governs a private cybersecurity investigator, it means section 25 of the Cybercrime Act is inconsistent with constitutional provisions. The participants also revealed that a lot of evidence that is presented in courts is obtained through unethical means, people's rights are violated in the process of obtaining that evidence and nobody talks about that. This is evident that section 25 of the Cybercrime Act has allowed that to happen by giving powers to individuals who are not members of SAPS and are not regulated by PSiRA as private investigators. It was

found that private cybercrime investigators are not even aware that private investigators are supposed to be registered with PSiRA, which is a huge concern that needs to be addressed.

## 6.6. The Requirements for Cybersecurity Specialist(s)

Within cybersecurity, there are various specialists. The requirements for specialising in specific cybersecurity roles are not determined by any law. A client determines who qualifies for a specific cybersecurity role. Employers use their experience and expertise in the field to develop job specifications. As aforementioned, there are different occupations within cybersecurity and each of them requires unique skills and/or qualifications. For instance, requirements for an ethical hacker or penetration tester differ from those of a forensic investigator or cybersecurity consultant, even though these are referred to as cybersecurity officers or specialists. The name, "cybersecurity officer" and/or "specialist" is very broad as it refers to any individual who renders security services in cyberspace, whether employed or self-employed. It is, therefore, impossible to uncover each requirement for cybersecurity roles. An employer of a cybersecurity officer determines the minimum requirements for any cybersecurity position. Some companies appoint an officer with a matric certificate and train them to be a cybersecurity officer. Others only appoint those with a post-matric certificate in different fields of cybersecurity. Usually, cybersecurity companies require internationally recognised qualifications.

There are cybersecurity roles that require specialists with a technical background, such as those with qualifications in IT, computer science, cybersecurity, or any related course. There is also an emphasis on a strong technical experience. Some companies require specialists to develop policies, which does not require any technical experience. A person with forensic investigation or any criminology degree may be useful if a company requires a specialist that can adduce evidence in a court of law.

It is important to note that there are no employment restrictions within cybersecurity as clients can hire a person from anywhere in the world. This is because there are no legislative requirements. This is different from the physical security environment, where it is categorically stated that only South Africans or permanent residents can render security services. Thus, in the cybersecurity space, geographical restrictions are not applicable. In some instances, companies would do background checks and that is possible with South African or permanent residents. The recruitment and/or contracting from other countries presents a regulatory challenge. For instance, a person who is not vetted may provide a

cybersecurity service in South Africa, thus compromising state security, especially where there is sensitive information involved.

### **6.7. The Sourcing of Cybersecurity Services**

There is a mixture of insourced and outsourced cybersecurity services. Most organisations prefer to outsource cybersecurity services to CSSPs, except the financial sector (the banks). Most banks can afford to insource cybersecurity services and afford to pay their cybersecurity specialists. The study found that there are various reasons behind the insourcing and outsourcing of cybersecurity services in the country. Since cybersecurity is a scarce skill and there is a shortage of cybersecurity specialists, insourcing is more expensive than outsourcing. An organisation that wants to create its own cybersecurity division needs to create a security operations centre, and should have the correct tools to operate, which is expensive. It is more cost-effective to appoint an MSSP than to build an internal cybersecurity team.

There are government departments that prefer outsourcing cybersecurity services to cybersecurity companies and require having these services provided on-site. This strategy enhances effective information management. State-Owned Entities (including critical infrastructures) also outsource cybersecurity services. The new industry is dominated by outsourced security companies.

### **6.8. The Requirements for a Cybersecurity Company**

There are arguably no regulatory requirements for a cybersecurity company to start operating. Anyone who meets the requirements of the Companies and Intellectual Property Commission (CIPC) on company registration can establish and operate a cybersecurity company. If the company staff has sufficient IT background and knowledge in cybersecurity or IT security, the company may market its services. The question of whether a company provides standard services rests with its client base. Clients would ascertain whether a company is aligned to international standards and bodies of knowledge that exist within the cybersecurity space before contracting a cybersecurity company.

### **6.9. The Certifications and Accreditation of Cybersecurity Training**

Employers of cybersecurity officers averred that they do check whether the officers have training from an industry-recognised institution. The majority of the preferred cybersecurity certificates are not offered by South African-based institutions. In South Africa, few public universities offer cybersecurity qualifications. There are also private institutions that offer cybersecurity training. Employers do not necessarily check whether an institution from where their employee was trained is accredited with any regulatory body in South Africa. If a candidate received a cybersecurity qualification from one of the highly preferred

institutions, the prospective employer would not hesitate to appoint the candidate as a cybersecurity officer.

It was noted that those who train at CISM are guaranteed of being hired by an audit firm and those who train at OSCP are guaranteed of being hired as pen testers.

The following are preferred cybersecurity qualifications and institutions, which guarantee very high chances of cybersecurity employment in South Africa.

QUALIFICATIONS	INSTITUTIONS
1. Certified Information Systems Security Professional	International Information System Security Certification Consortium – (ISC) <sup>2</sup>
2. Certificate in Cyber Security	University of Johannesburg (Centre for Cyber-Security).
3. CompTIA Security+	Computing Technology Industry Association – CompTIA
4. Certified Ethical Hacker	International Council of Electronic Commerce Consultants – EC-Council
5. Cybersecurity Fundamentals	Educor group
6. Certified Information Security Manager (CISM)	Information Systems Audit and Control Association – ISACA
7. Offensive Security Certified Professional (OSCP)	Offensive security
8. Microsoft cybersecurity certificate	Microsoft
9. Masters in Cybersecurity	University of Stellenbosch
10. Penetration testing, ethical hacking, SOC, etc.	CREST
11. And others	

Most of the above-listed qualifications are not necessarily offered by South African institutions and are expensive. Few companies accept matriculants and train them to be cybersecurity officers under the auspices of their skills programme. These companies prefer to teach their employees new skills.

Some employers have raised concerns regarding international qualifications that are not vetted. This brings another regulatory challenge as the legitimacy of these qualifications cannot be verified.

The appropriateness of training received by cybersecurity specialists is arguably determined by industry standards and requirements. There is, however, no standardised reference material. If one pursues training with one of the internationally recognised training institutions, employers assume that a person has received appropriate training. With this



training, employers have certain expectations. Some employers conduct skills evaluations to assess whether a would-be employee has the appropriate training.

### **6.9.1. The Exclusion of the Economically Disadvantaged in Cybersecurity Training**

It will be recalled that before 1994, certain classes of South Africans were excluded from pursuing certain qualifications based on various grounds, including race and gender. These classes of people are the so-called historically disadvantaged persons who became victims of unfair discrimination. In the cybersecurity space, it was found that cybersecurity training can only be accessed by those who are economically advantaged. Those who possess a certificate, diploma and degree in computer science, criminology, law, or any IT related qualification can only work in certain fields of cybersecurity locally and internationally, provided they are in possession of an additional internationally recognised certificate which comes at a huge cost. This creates a big challenge for an individual who has no means to fund cybersecurity training. The regulation of cybersecurity may provide opportunities for the economically disadvantaged to access cybersecurity training through several interventions, including the introduction of skills programmes for previously disadvantaged groups in the field of cybersecurity.

### **6.9.2. The Working Conditions within Cybersecurity**

Button (2020, p. 43) emphasised that cybersecurity officers, and in particular moderators, share common traits with physical security guards such as low pay, high labour turnover, and having to deal with incidents that take a psychological toll on them. Contrary to this assertion, the study found that cybersecurity officers are well taken care of, and their rights are respected. Since there is a shortage of cybersecurity specialists, employers treat them well, including paying them well. After all, cybersecurity is not confined to a certain geographical location, and cybersecurity officers can find a job anywhere in the world. Cybersecurity is internationally marketable.

As Button (2020) observed, cybersecurity companies must deal with high labour turnover. In the case of senior ethical hackers who are not more than 30 in South Africa, and must serve a lot of clients, the chances of them not staying for long with one employer are high. Due to the nature of their work, there is also a high turnover of MSSPs, especially the ones that work at cybersecurity operation centres. These are always working indoors monitoring signals from the deployed technology for 24 hours and 7 days a week.

The difference between cybersecurity officers and other employees is that they do not have trade unions. The working conditions of CSSPs are informed by the Basic Conditions of Employment Act 75 of 1997, meaning that they have the same employment rights and benefits as any other employees in the country. Most CSSPs use normal business hours,

which are from 08h00 to 17h00 - Monday to Friday. The exception is in relation to officers who provide managed security services because they work a 12-hour shift. There are no research studies on the working conditions of cybersecurity officers, which points to the need for studies to be undertaken in this area.

### **6.9.3. The Need for Regulation of Cybersecurity Services**

According to Button (2020, p. 50), “there is clearly a regulatory gap when the new private security industry is considered”. The study found that cybersecurity services are generally unregulated. There is a need for the regulation of cybersecurity in South Africa. This part focuses on the importance of regulating the new private security industry.

The regulation of the new private security industry is possible and the PSIR Act is relevant in this regard. While there are mixed views on the need to regulate the new industry, the study on the regulation of cybersecurity services in South Africa could not have been better timed.

Owing to the demand for cybersecurity, existing PSSPs are likely to transform their businesses to offer cybersecurity services. The private security industry sells “trust” to its end-users, which are clients, and if this trust is compromised, there is an inevitable loss of business. Before a client appoints a CSSP, assurance must be guaranteed on whether a prospective CSSP would have capabilities to safeguard and to respond to alerts in a timely and efficient manner. Therefore, the lack of regulated minimum standards creates an unfortunate “conducive environment” for incompetent service providers to operate in this space. It is for this reason, among others, that registration requirements (including minimum qualifications) are needed before a cybersecurity company and/or officer can be deemed as such.

The nonexistence of regulations results in many companies seeing cybersecurity as a business opportunity in their profit maximisation drive. This compromises professionalism in this space. This also introduces accountability challenges. CSSPs underscored the need for a designated regulator to provide oversight to their operations. The regulation of cybersecurity services and their providers will always be beneficial to the industry and the citizens in general. It is important to note that where there are regulations in place, professionalism is guaranteed. The nonexistence of specific regulations for cybersecurity services and their providers is also a weakness that cybercriminals have observed, and they are taking advantage of it. Many crimes occur in cyberspace, some of which are created by the fact that CSSPs are not regulated. There are also concerns relating to the issue of standardisation of cybersecurity services and the lack of quality services rendered thereof. It was found that there is huge uncertainty about the quality of services that CSSPs render to their clients.

There are some CSSPs that provide substandard services to their clients and the latter would not be able to pick this up. They only rely on word of mouth on which CSSP can provide the service. The existence of regulations would ensure that the company is accredited and can provide quality services. There are also international best practices and associations found within the industry. However, membership in these associations is voluntary and the best practices are not legally prescribed. Therefore, clients cannot always rely on whether a company is accredited by a voluntary institution. The need for regulation cannot be overemphasised to ensure the quality of services rendered in cybersecurity.

By way of example of the standardisation of services concerning the rendering of cybersecurity services, in the case of penetration testers, some penetration testers charge clients ridiculous amounts for one service. Their clients would pay because they need work done at a lower cost and overlook the work offered being substandard. Most clients that are not technically savvy do not have the capabilities of determining whether a penetration testing company will provide quality service. In the process, clients lose money as they are sometimes forced to contract another company to redo the work. Regulations become important in avoiding the use of unprofessional service providers.

The regulation of the new private security industry is important as there may be a possibility of industry opting for self-regulation, which may not necessarily be in the interest of the country. The formation of associations for purposes of self-regulation has its pros and cons. The main pro is that the industry arguably subjects itself to some form of control albeit not legally enforceable. In the case of cybersecurity, for instance, the associations would set and/or determine accreditation requirements for CSSPs. In the UK, there is an organisation called CREST, which is a non-profit accreditation and certification body that represents and supports the technical information security market (CREST, 2021). CREST provides internationally recognised accreditations for organisations and professional level certifications for individuals providing penetration testing, cyber incident response, threat intelligence and Security Operations Centre (SOC) services (CREST, 2021).

Once a CSSP is deemed by CREST to be fit and proper, most organisations feel safe to appoint CREST accredited companies because they have the knowledge that these providers went through rigorous tests before obtaining the certification. In South Africa, most banks hardly hire people or companies who are not CREST certified. CREST attempted to regulate CSSPs operating in South Africa but was met with resistance from the industry. Without regulations, the country's security will be compromised, and associations will emerge to seek to "regulate" the new industry.

As part of the regulatory regime, the designated regulator must accredit different cybersecurity training offered by CSSPs. Cybersecurity training institutions must be regulated. There is also a likelihood that cybersecurity training institutions attract candidates from all

over the world. Regulation of these institutions, including accrediting their training courses, will professionalise the industry. With the high level of unemployment in South Africa, it is hoped that this new private security industry will create employment opportunities, particularly for the South African youth.

One of the challenges envisaged in regulating this new industry is that most CSSPs operate in the digital world or space where they work remotely and where geographical restrictions are minimal. A cybersecurity company from anywhere in the world, for instance, can render a cybersecurity service to a South African-based company. In this way, certain categories can be effectively regulated in the country and also some cannot be easily regulated. It is more practically possible to regulate CSSPs in South Africa than those outside the South African borders. The viability or otherwise of regulating foreign cybersecurity companies rendering security services in South Africa remains to be seen.

As cybercrime and security measures change now and again, the regulation for cybersecurity needs to adapt to these changes. It is important to note that regulating the new industry will be informed by the dynamics and intricacies involved in this world of cyberspace. Such regulation cannot be an overnight project. While it may seem impossible, it is nevertheless achievable.

#### **6.9.4. The Legislation Relating to Cybersecurity**

Regulation must be understood within a broader context. First, there should be a determination made with regards to who can legitimately render security services in South Africa. A determination must be made by a specific entity established by national legislation. Second, there should be regulations and a code of conduct for CSSPs emanating from that legislation. To this end, CSSPs should be held legally responsible for contravening the law. Third, there should be punitive measures put in place for contravening the law. Fourth, there should be an enforcement capacity to ensure the effective regulation of the industry.

There are various laws and applicable standards in relation to cybersecurity, namely the Electronic Communications and Transactions Act 25 of 2002; Electronic Communication Act 36 of 2005; the Protection of Personal Information Act 4 of 2013; the Cybercrime Act 19 of 2020; and the Minimum Information Security Standards. These laws and standards are silent when it comes to the regulation of private cybersecurity services and their providers. It is important to note that cybersecurity and cybersecurity services are related but not the same. While cybersecurity is a generic term used to refer to the protection of cyberspace from cybercrimes, cybersecurity services refer to the security services used to protect cyberspace from cybercrimes.

*The Electronic Communications and Transactions Act 25 of 2002:* The purpose of the Electronic Communications and Transactions Act 25 of 2002 is to provide the facilitation and regulation of electronic communications and transactions; and development of a national e-strategy for the Republic of South Africa. This Act is silent about the regulation of cybersecurity services. It only establishes cyber inspectors who investigate matters that are in connection with what happens in cyberspace in general, not necessarily on aspects of cybersecurity services.

*The Electronic Communication Act 36 of 2005:* The Electronic Communication Act establishes a regulatory framework that is in line with technological and economic developments. It also promotes convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors. It also further provides for the legal framework for convergence of these sectors. Of interest, this Act only recognises security services provided in chapter 11 of the Constitution of the Republic.

Section 2(q) of the Electronic Communications Act provides that ICASA has a mandate to ensure information security and network reliability, which essentially means that information security service providers are allowed to operate but are arguably not regulated. The question of what qualifies the information security service providers if they are arguably not regulated is a subject of debate, which is beyond the scope of this study.

*The Cybercrime Act 19 of 2020:* It has been argued that the main reason for the existence of the Cybercrime Act is to make the internet a safer space for citizens and other people who live in South Africa. The Cybercrime Act 19 of 2020 prescribes cybercrimes and prescribes penalties for those offences. It imposes obligations on electronic communications service providers regarding the aspects that may impact cybersecurity. It must be noted that this Act does not provide for any regulations for cybersecurity services and their providers, but indirectly guides CSSPs' operations.

*The Protection of Personal Information Act 4 of 2013:* This Act regulates how personal information may be processed, stored, and shared. It essentially safeguards personal information. CSSPs who provide information security are guided by this legislation in so far as their operations are concerned. As Button (2020, p. 50) argued, "there is in most countries extensive regulation of data processing, but this does not cover all of the activities of the new private security industry and rarely creates deep licensing systems for personnel." The POPI Act regulates data processing and not necessarily CSSPs.

*The Private Security Industry Regulation Act 56 of 2001:* The PSIR Act provides for the regulation of the private security industry and establishes a regulatory authority for the private security industry, that is, PSiRA. The Authority's mandate is to regulate the private security industry and exercise effective control over the practice of the occupation of security

service providers in the public interest and national interest and the interest of the private security industry itself. There are regulations and a code of conduct for security service providers provided in terms of this Act. PSiRA is currently not regulating the rendering of security services in cyberspace.

*The Minimum Information Security Standards:* These standards are formulated only for information security services and their focus is on all institutions who handle sensitive information or classified material of the country. They are silent when it comes to the regulation of the rendering of cybersecurity services.

It was also found that South Africa's Internet Service Providers' Association (ISPA), which is a non-profit organisation and recognised internet industry representative body, monitors national cybersecurity developments and engages other industry bodies with cybersecurity programs, among other things. The primary role of ISPA is to serve as an active industry body, facilitating the exchange between the different independent ISPs, ICASA and other government structures, operators, and other service providers in South Africa. ISPA does not regulate internet security or cybersecurity. The ISPA security working group promotes online safety due to the vulnerability of their affiliates.

## 7. The PSIR Act and the Regulation of the Cybersecurity Industry

It is not disputed that cybersecurity services and their providers should be regulated by the Private Security Industry Regulation Act 56 of 2001 (PSIR Act). Chapter 2 of the PSIR Act provides for PSiRA's mandate to regulate this new private security industry. Section 1 of the PSIR Act defines security service as one of the following:

- (a) *Protecting or safeguarding a person or property in any manner.*
- (b) *Giving advice on the protection or safeguarding of a person or property, on any other type of security service as defined in this section, or on the use of security equipment.*
- (c) *Providing a reactive or response service in connection with the safeguarding of a person or property in any manner.*
- (d) *Providing a service aimed at ensuring order and safety on the premises used for sporting, recreational, entertainment or similar purposes.*
- (e) *Manufacturing, importing, distributing or advertising of monitoring devices contemplated in section 1 of the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992).*
- (f) *Performing the functions of a private investigator.*

- (g) *Providing security training or instruction to a security service provider or*
- (h) *Installing, servicing or repairing security equipment.*
- (i) *Monitoring signals or transmissions from electronic security equipment.*
- (j) *Performing the functions of a locksmith.*
- (k) *Making a person or the services of a person available, whether directly or prospective security service provider; indirectly, for the rendering of any service referred to in Paragraphs (a) to (j) and (l), to another person.*
- (l) *Managing, controlling or supervising the rendering of any of the services referred to in paragraphs (a) to (j).*
- m) *Creating the impression, in any manner, that one or more of the services in the paragraphs (a) to (l) are rendered.*

The comparison of CSSPs and PSSPs shows that CSSPs render almost all of the abovementioned security services in cyberspace for reward, remuneration, fee or benefit. PSiRA is only mandated to regulate PSSPs but also CSSPs. The “property” referred to in section 1 may be both physical and digital. Cyberspace is a space in which security services are and can be rendered and this does not limit PSiRA from executing its mandate concerning CSSPs. PSiRA should, therefore, ensure that all the objectives provided in section 3 of the Act are achieved in relation to this new industry.

This also means that section 20 of the PSIR Act must be applied to security service providers operating in cyberspace. In terms of the PSIR Act, CSSPs have a legal obligation to register with the Authority. For this registration to take place, relevant prescribed training requirements in respect of any category of security services (provided under section 21A) must have been complied with. This includes training requirements. Section 4(k) of the Act empowers the Authority to accredit all security training, which arguably includes cybersecurity training. As such, cybersecurity training providers and courses must be accredited by PSiRA. There is, therefore, a need to address this training requirement to be in line with the PSIR Act.

The PSIR Act provides that for one to be considered for registration, they must be a South African citizen or permanent resident. The same will be applicable to cybersecurity providers. Other requirements are found under section 23 of the PSIR Act that a security officer is only eligible for registration provided they have not been found guilty of an offence specified in the schedule within the period of 10 years immediately before the submission of the application to the Authority. Since the whole cybersecurity arrangement is not tangible, security equipment used in the physical space cannot be compared to that in the digital

space. The equipment includes software, which is used to protect and safeguard property or persons in cyberspace. It is important to note the role of the PSiR Act concerning the regulation of firewalls and intrusion detection software. Section 1 of the Act defines security equipment as a device used for intrusion detection, access control, fire detection, metal detection, x-ray inspection or for securing telephone communications. It may be argued that firewalls and intrusion detection systems in cybercrime form part of the definition of security equipment provided by the PSiR Act.

The regulation of the cybersecurity industry requires that the industry and its clients be aware of PSiRA, as the majority of CSSPs, as well as their clients, are not aware of PSiRA. The CSSPs highlighted it was their first time knowing about the Authority. They must understand their legal obligation of being PSiRA registered.

## 8. Recommendations

From this study, PSiRA arguably has a mandate to regulate the newly emerged private security industry. It is recommended that a legal opinion is solicited in order to determine the question around the legal mandate of PSiRA in regulating this industry. If established that the Authority has a mandate, cybersecurity services and its providers will have to be effectively regulated. This means the Authority will have to strengthen its efforts to regulate the cybersecurity industry, including bringing awareness to the public of its legal obligations towards the cybersecurity industry. This could involve a possible amendment of the current PSiR Act or the development of regulations specifically focusing on the cybersecurity industry. CSSPs rendering cybersecurity services within or outside South African borders must be registered with PSiRA. This also includes CSSPs that are not necessarily based in South Africa but provide cybersecurity services in the country.

It is recommended that for purposes of effectively regulating the cybersecurity industry, PSiRA should categorise the security services rendered in “cyberspace”. Service providers registered as PSSPs should only offer cybersecurity services once they also register as CSSPs. This is because the regulations applicable to CSSPs will differ from those of the PSSPs. It must be clear whether the security service providers are registered as PSSPs or CSSPs. The regulations must be meticulously drafted to regulate this new cybersecurity industry. It would be critical for the Authority to establish a committee representing all the PSiRA operational divisions that will be focusing on the development of these regulations.

As the current PSiRA grades are not in line with cybersecurity training, the Authority should consider aligning its training standards to accommodate those offered in cybersecurity. This will also include the accreditation of these standards. In line with its functions, the Authority must also consider developing cybersecurity training courses for CSSPs and prospective CSSPs. The Authority will have to apply to the South African Qualifications Authority (SAQA)



to be recognised as the professional body for the accreditation of cybersecurity qualifications in South Africa as empowered by section 4(k) of the PSIR Act. PSiRA should play a role in promoting cybersecurity training, particularly among the South African youth. To this end, establishing a partnership with the Department of Higher Education and Training as well as institutions of higher learning including universities and TVET colleges would be important and beneficial to the youth.

Most CSSPs have already obtained qualifications from various institutions. This must be considered in the drafting of the cybersecurity regulations, including the training regulations for CSSPs. To this end, it will be important for the Authority to develop and/or strengthen a working relationship with other regulators and government stakeholders responsible for cybersecurity, such as the ICASA, Information Regulator, State Security Agency and SAPS. Collaborations with other international bodies working on cybersecurity would be critical for the Authority to gain more knowledge on this new security industry. It is also recommended that PSiRA takes the lead in establishing an Association of Regulators in Africa to facilitate the exchange of best practices in the area of regulating cybersecurity in the continent. Through the association, international standards for the regulation of cybersecurity services can be developed.

As cybersecurity is a relatively novel phenomenon, strengthening research and development in this area cannot be overemphasised. Further research in this area must include international benchmarking to inform the drafting of the best possible regulations for the cybersecurity industry in South Africa. Furthermore, the PSiRA inspectorate must be strengthened to effectively monitor the rendering of cybersecurity. As the Authority is heading towards introducing a new funding model, this will be important for introducing new systems geared towards regulating the cybersecurity industry.

## 9. Conclusion

Cybersecurity, the new private security industry, has emerged alongside the traditional private security industry and is here to stay. Cybersecurity is arguably a security service in terms of the PSIR Act and must consider to be subjected to regulation by the Authority. The need for government to rethink and strategise on how to effectively regulate the cybersecurity industry in South Africa cannot be overemphasised. The regulation of the industry can only be effectively regulated provided its intricacies are well understood by the Authority. This study highlighted that the nature of criminal activities found in cyberspace, such as malware and ransomware, necessitate new security services in protecting cyberspace. These new services are different to those found in the physical space. Many security services under the auspices of cybersecurity are technology-driven due to the nature of cyberspace, which is intangible or rather digital. The most used cybersecurity measures are intrusion detection systems, firewalls, anti-viruses, and other anti-malware software.

The study highlighted that firewalls strictly deal with cyberattacks that emanate from the internet. They do not necessarily inspect and detect computer systems when access is gained as they cannot inspect and detect suspicious acts. Software developers designed firewalls by incorporating an intelligence layer on top of a firewall, which enables it to detect when access is gained by an unauthorised device. These firewalls send signals to the person responsible for safeguarding computer networks or systems. Antiviruses are designed to deal with malware that enters computer systems “manually”. An anti-virus checks for infected files and removes them before they disrupt, damage, or corrupt a system.

The study found that Internet Service Providers’ Association does not regulate internet security or cybersecurity. ISPA is a non-profit organisation and recognised internet industry representative body, which monitors national cybersecurity developments and engages other industry bodies with cybersecurity programs, among other things. Currently, there is no agency regulating the provision of cybersecurity services and their providers. It was found that security services rendered in cyberspace are arguably not unique to those offered in the physical realm. The only difference is the space in which the services are rendered. The intent of rendering such services remains the same. This informs the conclusion that cybersecurity services and their providers are part of the private security industry. It is for this reason that the study underscores the idea that CSSPs must be subjected to possible PSiRA regulation. However, a legal opinion has to be solicited in order to determine the question around the legal mandate of PSiRA in regulating the newly emerged industry. If established that the Authority has a mandate, cybersecurity services and its providers will have to be effectively regulated.

Since cybersecurity is more technical, the study recommends a possible new regulatory regime under auspices of the PSiR Act. For purposes of effectively regulating the cybersecurity industry, therefore, the study recommended that the Authority should strengthen its efforts within operations. This could involve championing the amendment of the current PSiR Act and/or drafting specific regulations that will focus on the cybersecurity industry. The new regulatory approach will ensure that foreign-based CSSPs rendering cybersecurity services within South Africa are also subjected to the PSiR Act.



## 10. References

- Abu-Taieh, E.M., 2017, November. Cyber Security body of knowledge. In 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2) (pp. 104-111). IEEE.
- Agarwal, H. and Agarwal, R., 2017. First Industrial Revolution and Second Industrial Revolution: Technological differences and the differences in banking and financing of the firms. *Saudi Journal of Humanities and Social Sciences*, 2(11), pp.1062-1066.
- Allen, J., Gabbard, D., May, C., Hayes, E. and Sledge, C., 2003. Outsourcing managed security services. CARNEGIE- MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
- Alqahtani, H., Sarker, I.H., Kalim, A., Hossain, S.M.M., Ikhtlaq, S. and Hossain, S., 2020, March. Cyber intrusion detection using machine learning classification techniques. In *International Conference on Computing Science, Communication and Security* (pp. 121-131). Springer, Singapore.
- Atkeson, A. and Kehoe, P.J., 2001. The transition to a new economy after the second industrial revolution (No. w8676). National Bureau of Economic Research.
- Bacudio, A.G., Yuan, X., Chu, B.T.B. and Jones, M., 2011. An overview of penetration testing. *International Journal of Network Security & Its Applications*, 3(6), p.19.
- Bertrand, C. and Bourdeau, L., 2010. Research interviews by Skype: A new data collection method. In *Paper Presented at the Proceedings of the 9th European Conference on Research Methodology for Business and Management Studies, Madrid, Spain*.
- Button, M., 2020. The new private security industry, the private policing of cyberspace and the regulatory questions. *Journal of Contemporary Criminal Justice*, 36(1), pp.39-55.
- Constitution, S.A., 1996. *The Constitution of the Republic of South Africa*.
- Craigien, D., Diakun-Thibault, N. and Purse, R., 2014. Defining cybersecurity. *Technology Innovation Management Review*, 4(10).
- CREST, 2021. CREST - Assurance in Information Security. Crest-approved.org. Available at: <https://crest-approved.org/> [Accessed 19 December 2021].
- Cybercrime Act 19 of 2020. Available at: [https://www.gov.za/sites/default/files/gcis\\_document/202106/44651gon324.pdf](https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf)

- De Vries, J., 2013. *European Urbanization, 1500-1800*. Routledge.
- Deane, P.M., 1979. *The first industrial revolution*. Cambridge University Press.
- Ding, W., Yurcik, W. and Yin, X., 2005, December. Outsourcing internet security: Economic analysis of incentives for managed security service providers. In *International Workshop on Internet and Network Economics* (pp. 947-958). Springer, Berlin, Heidelberg.
- 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.
- Dlamini, S. and Mbambo, C., 2019. Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social sciences*, 5(1). p. 1675404.
- Dubois, J. and Jreije, P., 2006. Mechanisms of internet security attacks. *Transactions on Engineering, Computing, and Technology*, pp.166-168.
- Electronic communications Act 36 of 2005. Available at: [https://www.gov.za/sites/default/files/gcis\\_document/201409/a36-050.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/a36-050.pdf) (Accessed: 09 December 2021).
- Electronic Communications and Transactions Act 25 of 2002. Available at: [https://www.gov.za/sites/default/files/gcis\\_document/201409/a25-02.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf)
- Fox, S.J., 2016. Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism. *Journal of transportation security*, 9(3), pp.191-218.
- Furnell, S., 2003, July. Cybercrime: vandalizing the information society. In *International Conference on Web Engineering* (pp. 8-16). Springer, Berlin, Heidelberg.
- Gollin, D., Jedwab, R. and Vollrath, D., 2016. Urbanization with and without industrialization. *Journal of Economic Growth*, 21(1), pp.35-70.
- Harper, M. and Cole, P., 2012. Member checking: Can benefits be gained similar to group therapy. *The qualitative report*, 17(2), pp.510-517.
- International Civil Aviation Organization., (2021). *Civil Aviation Cybersecurity*. Available at: <https://www.icao.int/cybersecurity/Pages/default.aspx> (Accessed: 1 July 2021).
- Janicke, M. and Jacob, K., 2013. A third industrial revolution. Long-term governance for social-ecological change, pp.47-71.

- Johnson (2021). *Worldwide digital population as of January 2021*. Statista. Available at: <https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=How%20many%20people%20use%20the,the%20internet%20via%20mobile%20devices> (Accessed: 19 May 2021).
- Jones, S.L., Collins, E.I., Levordashka, A., Muir, K. and Joinson, A., 2019, May. What is 'Cyber Security'? Differential Language of Cyber Security Across the Lifespan. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-6).
- Kolb, M., 2018. *What is globalization: And how has the global economy shaped the United States*. Peterson Institute for International Economics. Available at: <https://www.piie.com/microsites/globalization/what-is-globalization> (Accessed on: 5 July 2021).
- Landreneau, K.J. and Creek, W., 2009. *Sampling strategies*. Available at: <http://www.natco1.org>.
- Lewis, J.A., 2006. *Cybersecurity and critical infrastructure protection*. Center for Strategic and International Studies.
- Mathias, P., 2013. *The first industrial nation: The economic history of Britain 1700–1914*. Routledge.
- Mazzotta, G., 2018. *Toward live memory forensics for malware identification*.
- Mchunu, V., 2021. *Cyberattack threatens SA's national security*. Available at: <https://www.iol.co.za/mercury/news/cyberattack-threatens-sas-national-security-5903bc24-5bbd-483e-a46e-17c080490633> (Accessed: 09 November 2021).
- Minnaar, A. and Ngoveni, P., 2004. *The relationship between the South African Police Service and the private security industry: any role for outsourcing in the prevention of crime?*. *Acta Criminologica: African Journal of Criminology & Victimology*, 17(1), pp.42-65.
- Mohurle, S. and Patil, M., 2017. *A brief study of wannacry threat: Ransomware attack 2017*. *International Journal of Advanced Research in Computer Science*, 8(5), pp.1938-1940.
- Nadikattu, R.R., 2020. *New Ways of Implementing Cyber Security to Help in Protecting America*. *Journal of Xidian University*, 14(5), pp.6004-6015.
- Oppliger, R., 1997. *Internet security: firewalls and beyond*. *Communications of the ACM*, 40(5), pp.92-102.

- Pang, K., n.d. *Maritime Cyber Security: The Emerging Virtual Threat to Shipping*.
- Pedley, D., Borges, T., Bollen, A., Shah, J.N., Donaldson, S., Furnell, S. and Crozier, D., 2020. *Cyber security skills in the UK labour market 2020*.
- Private Security Industry Regulation Act 56 of 2001.
- Radulov, N., 2019. *Security 4.0. Part one: Security and the fourth industrial revolution. Industry 4.0, 4(5), pp.265-267*.
- Roberts, B., 2015. *The third industrial revolution: implications for planning cities and regions. Work. Pap. Urban Front, 1*.
- Rowe, B., Reeves, D. and Gallaher, M., 2009. *The role of internet service providers in cyber security. Institute for Homeland Security Solutions*.
- Saadat, F. and Soltanifar, M., 2014. *The Role of Internet Service Providers (ISPS) in Encouraging Customers to Use Their Internet Services in Iran. International Journal of Business and Social Science, 5(3)*.
- Schwab, K., 2017. *The fourth industrial revolution. Currency*.
- 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.psir.co.za/dmdocuments/research/2021/PSiRA%20Report%20Airport%2001%20\(003\).pdf](https://www.psir.co.za/dmdocuments/research/2021/PSiRA%20Report%20Airport%2001%20(003).pdf) (Accessed: 10 July 2021)*.
- Siboni, G. and Sivan-Sevilla, I., 2017. *Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations*.
- Soh, M.B.C., 2012. *Crime and urbanization: Revisited Malaysian case. Procedia-Social and Behavioral Sciences, 42, pp.291-299*.
- Stevenson, A. ed., 2010. *Oxford Dictionary of English. Oxford University Press, USA*.
- 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*.
- Von Solms, R. and Van Niekerk, J., 2013. *From information security to cyber security. computers & security, 38, pp.97- 102*.
- Xu, M., David, J.M. and Kim, S.H., 2018. *The fourth industrial revolution: Opportunities and challenges. International journal of financial research, 9(2), pp.90-95*.


- 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> (Accessed: 23/2021).
- Yar, M., 2005. *The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory*. *European Journal of Criminology*, 2(4), pp.407-427.
- Zama, N., 2020. *Securing the Seafare: Regulating the Private Maritime Security Industry in South Africa*. Available at: <https://www.psira.co.za/dmdocuments/research/2021/PSiRA%20Report%20Maritime%2001.pdf> (Accessed: 23 May 2021).











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

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

**Email :** [info@psira.co.za](mailto:info@psira.co.za)

**Website:** [www.psira.co.za](http://www.psira.co.za)

 Private Security Industry Regulatory Authority  
 082 803 4329  
 Psiralive