



**PSiRA**  
Private Security Industry Regulatory Authority

**A NEW DAWN:  
The Impact of the  
4IR on South Africa's  
Private Security  
Industry**



## About the Report

**Title:** A NEW DAWN: The Impact of the 4IR on South Africa's Private Security Industry

**Author:** Londiwe Caluza

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

**Year Published:** 2022

**Special Thanks:**

Arial Works  
QP Drones  
Hikvision  
Wise Guys  
Spartan  
Impumelelo Security Training  
Empower Training Centre  
The South African Security Training Academy  
Mgwambani Security and Projects  
The National Gambling Board  
Ghost Security  
PSiRA Law Enforcement and PSiRA Legal Department



**PSiRA**  
Private Security Industry Regulatory Authority



## ABBREVIATIONS AND ACRONYMS

<b>2IR</b>	Second Industrial Revolution
<b>3IR</b>	Third Industrial Revolution
<b>4IR</b>	Fourth Industrial Revolution
<b>AI</b>	Artificial Intelligence
<b>App</b>	Application Software
<b>BEE</b>	Black Economic Empowerment
<b>CAA</b>	Civil Aviation Authority
<b>CCTV</b>	Closed-Circuit Television
<b>COVID-19</b>	Novel Coronavirus Disease 2019
<b>IoT</b>	Internet of Things
<b>IR</b>	Industrial Revolution
<b>IRSA</b>	Information Regulator South Africa
<b>NBR</b>	National Building Regulator
<b>NGB</b>	National Gambling Board
<b>PI</b>	Private Investigator
<b>PSiRA</b>	Private Security Industry Regulatory Authority
<b>ROC</b>	Remotely Piloted Aircraft System Operating Certificate
<b>RPL</b>	Remote Pilot License
<b>SACAA</b>	South African Civil Aviation Authority
<b>SASSETA</b>	Safety and Security Sector Education and Training Authority
<b>SETA</b>	Sector Education and Training Authority
<b>SIA</b>	Security Industry Authority
<b>UK</b>	United Kingdom
<b>USA</b>	United States of America



# Table of Contents

<b>Abbreviations and acronyms</b> .....	<b>III</b>
<b>Executive Summary</b> .....	<b>1</b>
1. Introduction.....	2
2. Background of the Study.....	2
3. Research Aim and Objectives.....	3
4. Research Hypothesis and Questions .....	4
5. Research Methodology.....	4
6. Research Limitations.....	5
7. Literature Review .....	5
7.1 The History of Industrial Revolutions.....	6
7.2 Defining the 4IR .....	6
7.3 The Technologies of the 4IR .....	7
7.4 Regulating the 4IR Technology within the Private Security Industry.....	14
8. Research Findings.....	18
8.1 Challenges and Opportunities of the 4IR.....	18
8.2 Training in the 4IR.....	22
8.3 “TRANSFORMATION” in the Industry.....	27
8.4 Adopting Best Practices Locally and Internationally.....	28
8.5 Regulating the Private Security Industry .....	29
9. Recommendations.....	32
9.1 Security Equipment.....	32
9.2 Best Practices .....	33
9.3 PSiRA Communication, Training and Registration Unit.....	33
9.4 Implementing Research Recommendations .....	34
9.5 Mandatory Skills Development .....	35
9.6 PSiRA Partnerships.....	35
10. Conclusion.....	35
11. References.....	37



## EXECUTIVE SUMMARY

Indeed, a new dawn is upon us, disrupting how people engage with technology. The COVID-19 pandemic is probably one of the factors that propelled the world at large to embrace the new technologies of the 4IR. Just like any other industry, private security is impacted by the changes of the 4IR. Hence this study was conducted to explore the impact of the 4IR on South Africa's private security industry.

The study aims to explore the role of PSiRA as the regulator of the private security industry in South Africa towards the unfolding 4IR technology. This was done by exploring the challenges and opportunities being brought by the 4IR to the private security industry; exploring the relevance of the PSIR Act 2001 towards the 4IR and exploring the best practices in regulating 4IR technology in the private security industry. The report also sought to discover the required training standards for the use of 4IR technology in the industry and to determine which technologies PSiRA can utilise in regulating the industry.

From the data collected, it was established that the 4IR brought about a new field within the private security industry, known as aerial security. This new field has the potential to mitigate any job losses that will be brought about by the 4IR. The study established a need for the Authority to develop sector-specific training standards. Although the PSiRA grades are still relevant, they are arguably not applicable to other sectors in the industry. The report also highlights the need to regulate security equipment as more and more security companies are adopting these new technologies. These equipment(s) process highly sensitive personal information and their use must be regulated. Several recommendations from the industry are included in the report and include the adoption of best practices from other organisations when it comes to regulation in the 4IR and establishing standards to be used when regulating security equipment.

## 1. Introduction

At the essence of human existence is the need to continuously evolve in the quest to improve the way of life. The industrial revolutions that have unfolded throughout history are evidence of this. Some may argue that the industrial revolutions are more focused on the means of production. However, with the Fourth Industrial Revolution (4IR) many other businesses and institutions are finding themselves having to embrace the 4IR.

The 2019 Novel Coronavirus (COVID-19) is probably the biggest cause of fast-tracking the 4IR and the use of its technologies. From micro- to macro-level, the impact of COVID-19 can be felt and there is an overwhelming need to embrace the 4IR now more than ever. During the launch of the virus aid plan at a UN conference, author and commentator of the digital revolution, Keen, said that “the digital world, however, is thriving. We are surviving through this pandemic because of technology” (Rasheed, 2020).

There are fears that the 4IR may do more damage than good, especially in Third World countries. Africa as a continent has lagged in past industrial revolutions and so far, it still lags in several indicators essential for a successful digital revolution (Ngung’u and Signe, 2020). Be that as it may, this lag also provides an opportunity for growth and reform of businesses and entities, which they will steer at the helm, especially when it comes to the reinvention and creation of labour and skills.

Undoubtedly, the 4IR already has impacted the private security industry. As to how severe the impact is and how much change it will bring to the industry, its regulation still needs to be investigated. The Private Security Industry Regulatory Authority (PSiRA) is mandated to regulate the industry and to exercise effective control over the occupation of the security service provider in the public and national interest and the interest of the private security industry itself (PSiRA Act, 2001). There is a need for the Authority to explore the effects of the 4IR, particularly on different sectors of the industry. Moreover, the Authority needs to establish if the existing regulations are applicable and sufficient to regulate the private security industry in this new era.

## 2. Background of the Study

The introduction of technology to societies has led to many changes in their standards of living. Ever since the inception of the First Industrial Revolution until the Third Industrial Revolution, there were no major changes witnessed but unlike those brought by the 4IR. It was very recently when Klaus Schwab introduced the concept of 4IR. The rapid pace and major changes that the 4IR comes with cannot be ignored. There is a lot of uncertainty on how it will continue to unfold. Be that as it may, one thing is clear: the response to it





must be integrated and comprehensive, involving many stakeholders of the global polity, from the public and private sectors to academia and civil society. The era is evolving at an exponential rather than linear pace. Aptly, this will require industries to be knowledgeable about the effects of the 4IR on their daily operations.

As previously mentioned, the 4IR is already impacting the private security industry. The use of technology in the industry is not new, however, the latest technology is more advanced, and it brings along great uncertainty and opportunities. As it stands, the existing 4IR technology is disrupting the status quo of how things are normally done. Some security companies have started using drones for patrolling. It was found that drones made it possible for anti-poachers to patrol areas faster (Caluza, 2020). In the US, the Knightscope K5 Robot was created to offer car-guarding services and can read 300 number plates in a minute using Artificial Intelligence (AI) (Nanalyze, 2017). Closed-circuit television (CCTV), which has been used for years in the private security industry also uses 4IR technology, with some of these CCTVs being used for predictive policing. Apart from the expected job losses due to the 4IR, there are also concerns about violation of human rights, particularly issues around discrimination and the right to privacy. The study also looks into existing legislation, locally and internationally, that regulates the 4IR technology as found within the private security industry.

### **3. Research Aim and Objectives**

This study aims to explore the role of PSiRA as the regulator of the private security industry in South Africa towards the unfolding 4IR technology.

The objectives of the study are as follows:

- To explore the challenges and opportunities being brought by the 4IR to the private security industry.
- To explore the relevance of the PSIR Act, 2001 towards the 4IR.
- To explore the best practices in regulating 4IR technology in the private security industry.
- To discover the required training standards for the use of 4IR technology in the industry.
- To determine which technologies PSiRA can utilize in regulating the industry.

## 4. Research Hypothesis and Questions

The hypothesis of this study is as follows: *The technology brought about by the 4IR is impacting on the private security industry and regulation(s) thereof.*

The primary research question is: *What role will PSiRA play as the regulator towards the 4IR?*

The secondary research questions are as follows:

- What are the possible challenges and opportunities of the 4IR towards the private security industry?
- What are the current regulatory mechanisms used to regulate the 4IR technology?
- How will the introduction of the 4IR affect the current security training standards?
- What technologies can PSiRA use in regulating the industry?

## 5. Research Methodology

According to Kothari (2004), research methodology can be understood as a scientific study of how the research will be conducted or as a systemic way of solving a problem. This part will discuss the research procedures or techniques that will be employed to identify, select, process and analyse data about the 4IR. The study seeks to discover the reality of the effects of the 4IR in the private security industry. Therefore, the study will adopt an interpretivism research paradigm. Thanh and Thanh (2015) believe that reality is socially constructed, meaning that researchers need to understand the phenomenon being studied through participants' perceptions and experiences in that particular sector. The answers of the research in the interpretivism paradigm are received from the experiences of the participants and the researchers must construct and interpret the understanding of the gathered data (Thanh and Thanh, 2015).

The research will use a methodology that will provide an in-depth understanding of the topic. In this case, a qualitative approach will be selected. Creswell (2009) defines this approach as a way of exploring and understanding views of the individuals or groups that ascribe to the research problem. The qualitative research approach will allow the private security industry and the regulators to express their lived experiences in various aspects of the 4IR. The research will use face-to-face interviews and observation as data collection instruments from the qualitative approach. The interviews will involve the use of a semi-structured questionnaire; this type of questionnaire provides a set of open-ended questions

that may allow a follow-up question if there is an unclear statement made by the participant. The observations will be used to gain insights into how security equipment is used.

The sample of the study consists of regulators, equipment sellers, manufacturers and consumers of the 4IR security equipment, and security officers. The study will use snowball and purposive sampling methods. Tangco (2009) defines purposive sampling as a non-random sampling that selects participants on the qualities they possess. Goodman (1961) referred to snowball sampling as a method wherein participants refer a researcher to another participant(s). Using the snowballing sampling method will ensure that the precise participants are sampled and will be able to give the correct information for this research.

## 6. Research Limitations

With the advent of COVID-19, there were obvious uncertainties as to whether or not there would be travel restrictions in place during data collection. This potentially could have an impact on the number of research participants for the study. From previous experience, using virtual meetings had its limitations because not everyone uses these platforms. However, more people are using these platforms as a preventative measure to prevent the spread of COVID-19. Virtual meetings and telephonic interviews were also used during the data collection period when participants were unable to have face to face interviews.

## 7. Literature Review

This section presents the literature review, which will review existing literature on the 4IR. Terre Blanch, Durkheim and Painter (2006) describe literature review as the “identification and analysis or review of the literature and information related to what is being intended to be, or has been, studied”. This literature will assist with the information that previous studies discovered. Previous publications have much more to contribute to the study and therefore its utilisation will help to advance the study. Moreover, it will also provide a scientific background to the study and will assist with the identification of gaps that exist within the pool of knowledge.

Firstly, this part will provide a background of previous industrial revolutions and define the 4IR. This will assist in highlighting the importance of studying the impact of this Industrial Revolution as it is affecting every industry and individual globally. Secondly, it will highlight the different technologies of the 4IR. Due to the vast technologies that already exist, only technologies used in the private security industry will be mentioned. Lastly, this part will present a discussion on the laws and policies regulating the 4IR locally and globally.

## 7.1 The History of Industrial Revolutions

Before highlighting the history of industrial revolutions, it is important to first understand what an industrial revolution is. According to Vries (2008), an industrial revolution is the development that occurs when there is a transition from one industrial society to the other. The Merriam-Webster Dictionary (2021) describes an industrial revolution as being “a major change in the economy marked by the general introduction of power-driven machinery or by an important change in the prevailing types and methods of use of such machines”. Industrialisation is also characterised by the social change it brings to society.

The Industrial Revolution (IR) is recorded to have started in the 18th century with its origins being from Britain and later spreading to the rest of the world. The IR in Britain and Western countries was centred around the change of human and animal use in production to the use of machinery and steam engines (Mohan, 2019). The Second Industrial Revolution (2IR) was characterised by the advancements of machinery from the IR and the use of electricity during 1870 and 1914 (Noble, 2020). The Third Industrial Revolution (3IR) brought about the era of digitisation during the 1980s (Noble, 2020).

In South Africa, the IR was different as it was centred around the discovery of minerals in the late 1800s (Potenza, 2012). The industrial revolutions that unfolded in the Western countries also unfolded in South Africa. However, South Africa just like other 2nd and 3rd world countries developed later, resulting in a lag in their development. An article by van Eck (1951) analysing the IR and the 2IR states that “the development of such a society must inevitably be gradual as no nation can pass directly in a short time from a simple and primitive economy to a complicated one”. One of the biggest concerns with the current 4IR is the lag in technology which the country needs to cover (Noble, 2012). Secondly, the previous industrial revolutions have resulted in job losses, especially for those who are not educated (Noble, 2012). As it stands, the unemployment rate in the country stands at 32,6%, the highest it has been since 2008 (Writer, 2021). Moreover, the COVID-19 pandemic has left many capable workers unable to work (Writer, 2021).

## 7.2 Defining the 4IR

The concept of 4IR was first coined by Professor Klaus Schwab. As to the existence of a single universal definition of the 4IR, none exists now. However, some articles (Schwab, 2016; Schwab, 2017; Xu, David, and Kim, 2018) suggest that it is the advancement of the 3IR, which was more into the use of electronics and information technology for production. The 4IR consists of three spheres, namely the physical, digital and biological spheres (Xu *et al.*, 2018) which merge because of the new technologies brought about by the 4IR. The merger of these three spheres has impacted all disciplines, economies and industries that exist.

Schwab (2017) argues that the way technology is unfolding might have some implications on human life. Moreover, the scale, scope, and complexity of the 4IR will be very different to what human beings have experienced before (2017). This technology is already visible in workspaces, homes, schools and even with our electronic devices such as laptops, cell phones, appliances and cars (UJ, 2021).

The 4IR comes with great promise and great peril. It comes with great promise as it can connect billions of people through digital networks. It can improve the efficiency of organisations and assist with asset management with organisations not having to use the traditional method of doing things (Schwab, 2017). This will assist in regenerating the natural environment and potentially undoing the damage of previous industrial revolutions (Schwab, 2017). It comes with great peril as organisations might not be able to adapt and governments not being able to employ and regulate new technologies (Schwab, 2017). Moreover, not being able to capture the benefits of these technologies will lead to inequality and societies fragmenting (Schwab, 2017).

### **7.3 The Technologies of the 4IR**

As aforementioned, this part of the literature review will focus on the 4IR technologies used within the private security industry. The technologies to be discussed will be from the physical and digital spheres. The biological sphere will not be discussed as it is uncertain how the biological sphere affects the private security industry, and it has not received much attention from scholars who conduct research on the private security industry. This study will discuss how it affects the private security industry.

#### **7.3.1 The Digital Sphere**

##### **7.3.1.1 Artificial Intelligence and Machine Learning**

The concept of artificial intelligence (AI) was derived from the seminal work of Alan Turing on Computing Machinery and Intelligence in the 1950s (IBM Cloud Education, 2020). Marvin Minsky and John McCarthy, who are said to be the fathers of the field, later coined the concept of AI. They described AI as any task performed by a machine that would have previously been considered to require human intelligence (Heath, 2020). Many definitions of what is AI exist; however, Carter (2019) describes AI as the mechanism that enables machines to learn, which will make them adjust to the environment they are put in and perform a task without human intervention in making decisions.

Two types of AI exist, namely narrow or weak AI and general or strong AI. Machines that use weak AI are those that cannot self-operate and require human intervention. However, those machines can still outsmart human beings in some tasks (Lu, Li, Chen, Kim and Serikawa,

2018). An example of weak AI is a computer. The strong AI is merely a modification of the weak AI. Machines with strong AI technology can think and make decisions independently without human intervention (al-Rifaie and Bishop, 2015). The general AI design was made to outperform human beings concerning their cognitive tasks (Lu *et al.*, 2018).

For machines to operate independently, they need to learn (Vu, 2018). Mohammed, Khan and Bashier (2016) state that machines alone cannot have the ability to learn and make decisions, therefore, there should be an element of AI called machine learning that has to be installed, which enables machines to perform their tasks independently. Reinharz (2019) defines machine learning as the capability of the installed software to recognise patterns on the collected data. Machine learning makes the machines operate in complex situations. The disadvantage of machine learning, however, is that the programmers do not have an idea of how the machines react when they encounter situations that are outside their programmed parameters.

Mohammed *et al.* (2016) highlight that the machines gather information through senses that are like those of human beings, such as sight and hearing. The data from the previously mentioned senses is then processed using the intelligence of a computer, which will inform decision-making that is like that of human beings (Mohammed *et al.*, 2016). The pattern recognition algorithms form part of the categories of AI. The technology would be incorporated in the autonomous unmanned systems such as boom gates with number plate recognition cameras that open for registered number plates in business parks or estates.

AI and machine learning are quickly transforming the security landscape, forcing the industry to re-evaluate their traditional ways of doing things. Security equipment such as Close Circuit Television (CCTV) now have AI unlocking new functionalities, and even changing the role CCTV plays for companies (Lindsey and Woolf, 2021). AI technology is not only limited to CCTV but other security equipment such as drones also use AI technology. Seemingly this technology has led to security professionals re-imagining how they'll build their teams, structure engagements and define their value (Lindsey and Woolf, 2021). This has already materialised with security companies establishing new units within their companies. One of the biggest security companies in South Africa has introduced drone response as one of their security services (Coetzee, 2021).

### 7.3.1.2 Internet of Things

In 1999, entrepreneur Kevin Ashton formulated the concept of Internet of Things (IoT) (SAS Insights, 2021). IoT connected devices communicate via networks or cloud-based platforms connected to the IoT (SAS Insights, 2021). Cloud refers to servers that are accessed over the internet, and the software and databases that run on those servers and storage takes place on servers in a data centre, instead of locally on the user device (Cloudflare, 2021).



Dobre (2017) refers to IoT as the connectivity of digital devices to the internet with the aim of interacting with each other without human intervention. These devices include sensors, actuators, laptops, tablets, digital cameras, smartphones, alarms systems, home appliances, industrial machines and other personal electronic devices.

Johnson (2019) and Dobre (2017) argue that IoT technology came with smart cameras (consisting of object recognition technology) that monitor premises. These cameras do not require human intervention to analyse and alert authorities when a security breach has been detected, they do so automatically. Dobre (2017) states that the introduction of these smart cameras led to the connectivity of sensors to the cameras. The sensors in the cameras detect changes in environmental variables (movements or temperature) and send a signal to the cameras so that they would start to capture everything in that location (Dobre, 2017). The same applies to incidents that occur at night where cameras, building lights and sensors that are connected to a computer will react should anything suspicious be detected. The lights will automatically switch on and the cameras will begin to capture everything that is happening in that place (Dobre, 2017). Similar technology is used in alarm response, if an alarm system is activated, the cameras, sensors and computers will start to operate simultaneously (Dobre, 2017).

IoT technology has its benefits and its disadvantages for the private security industry. IoT Technology will arguably lead to job losses, even though it will not eliminate the need for on-site security provision (Johnson, 2019). The use of IoT will change how security officers carry out their work. The duties of security officers will be less monotonous and be more effective as they will not have to monitor screens for hours. This means that security officers can do other meaningful things during that time (Johnson, 2019). Dobre (2017) argues that the significant part of this technology is that human intervention in monitoring security equipment will not be of importance due to the automation of the security equipment. Johnson (2019) further argues that IoT will reinforce private security, meaning it will not replace security officers but the two will work together to maximise the protection of people and properties.

### **7.3.2 The Physical Sphere**

#### **7.3.2.1 Robotics Providing Security in the 4IR**

One of the anticipated developments of the 4IR is the creation of more highly digitised robots that will provide a security service. As it stands, the use of robots in the security industry is already at play with some companies in some of the First World countries having employed robots to provide security services in and around buildings and some even in public spaces (Gonzalez, 2017). This part of the literature review will look at robots, more specifically ground and aerial security robots, that have been developed to provide security services.

### 7.3.2.2 Definition of Robotics and Robots

Before going in-depth with the literature, it is of cardinal importance to first unpack what robotics is to appreciate what robotics and robots are. Robotics is an interdisciplinary branch of engineering and science that includes mechanical and electrical engineering, computer science, and other fields in science (Khan and Khan, 2017). Moreover, robotics deals with the design, construction, operation, and use of robots, as well as computer systems for their control, sensory feedback, and information processing (Khan and Khan, 2017). In short, robotics deals with the technological aspects of the robot.

On the other hand, a robot is a machine programmed by a computer, enabling it to carry out complex series of actions automatically (Oxford English Dictionary, 2021). There are three components that a robot needs to meet before being deemed as a robot. Aptly, it must be able to interact with the world using sensors and actuators, it must be programmable, and lastly, it must be autonomous or semi-autonomous (Hill, 2017). These elements interrelate with each other to ensure the functioning of the robot. To ensure that this happens, the robot needs to be programmed so that it functions. Programming is the analysis, the generating of algorithm accuracy (a set of instructions designed to perform a specific task) (Tech Terms Dictionary, n.d.) and resource consumption, and implementation of algorithms through coding (the process of using a programming language to get a computer to behave how you want it to) (Bebbington, 2014). The purpose of this is to find a sequence of instructions that will automate (the technology by which a process or procedure is performed with minimal human assistance) (Mikell, 2014) the performance of a task (Bebbington, 2014), and that task being whatever function the end-user of the robot may need it to function. It is important to note that without programming, a robot has no use to the end-user who needs it to perform certain tasks.

### 7.3.2.3 Ground and Aerial Security Robots

In a gist, the 4IR is the distortion of boundaries that exist between the digital, physical and biological worlds with new technologies emerging from this phenomenon (Vu, 2018). Robotics, which falls under the physical spectrum of the 4IR, is fast gaining momentum in growth mainly because it could well be one of the core aspects of the 4IR. Moreover, robots have already been in use especially in the manufacturing sector (Hill, 2017) for some time to increase manufacturing productivity.

Although the idea of robots is not new, their ever-increasing capacity and autonomy are (Joh, 2017). The functions that robots perform were merely a figment, but the technology used in programming these robots has made it possible for them to become a reality. Yelp, which is an American owned security company, has developed a state of the art robot



named Cobalt. Cobalt was created to provide security services whereas other robots that have been developed provide concierge services in hotels, do stocktaking in warehouses, and give out medicine and food in hospitals (Gonzalez, 2017).

Cobalt is a patrolling robot that has a 95% accuracy rate for identifying anomalies and can read situations, people and objects to evaluate whether or not they belong (Nanalyze, 2017). Although it is an autonomous robot, it still requires human assistance. When an anomaly has occurred, the robot sends a signal to a human counterpart for them to evaluate the situation themselves (Gonzalez, 2017). Cobalt and other security robots are a complement to the work done by security guards and their technological advancements make it possible for this to happen. Cobalt uses AI, machine learning and computer-vision algorithms to recognise people, places and temperature deltas (Gonzalez, 2017). The Knightscope K5 robot, which is a parking lot monitor, uses AI as well to read nearly 300 number plates on cars in a minute (Nanalyze, 2017). Just like Cobalt, the K5 sends out a signal to the authorities or its owner when it detects something abnormal.

Aerial robots have emerged in the form of drones and other lightweight driverless planes. Drones have become very popular not only in the security industry but in other industries as well. The ability to go into spaces that humans may not be able to infiltrate gives drones an advantage (Nanalyze, 2017). Drones, formerly known as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASes), are flying robots that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems (Earls, Shea and Wigmore, n.d.). These systems work in conjunction with onboard sensors and GPS (Earls, Shea and Wigmore, n.d.). Just like any robot, drones need to be programmed to function. The same technology found in ground robots is found in drones or aerial robots.

SECOM, which is Japan's biggest security company, launched its security drone in 2015. The drone can chase down and follow people without human intervention (Williams, 2015). The drone is a complementary security equipment that launches to the site whenever suspicious cars or people are detected on the property by other security equipment (Williams, 2015). Unlike conventional surveillance cameras, drones are a promoted security equipment alternative because of their ability to fly anywhere on a property and take pictures of people and objects from different angles (Williams, 2015). Drones have also been in use in South Africa's private security industry. PSiRA studies by Caluza (2020) and Caluza and Zama (2020) highlight the use of drone's security officers in providing private security services. Security companies have also introduced drone technology in residential areas to combat crime in Johannesburg (Daniel, 2021).

Singapore based company Otsaw Digital has also developed a drone called the O-R3, which is dubbed the “world’s first ground-aerial outdoor security robot” (Nanalyze, 2017). The drone is a dynamic duo with a self-driving vehicle with 4-wheel drive and a drone to break out of the sticky spots the vehicle cannot reach (Nanalyze, 2017). Dubai plans to have these robots make up 25% of the police force by 2030 (Nanalyze, 2017).

Drones are also being used in the law enforcement and military space. In the USA, they are used for search and rescue missions, traffic collision reconstruction, crime analysis, surveillance, crowd monitoring and investigations of active shooters or suspects (Margaritoff, 2017). The use of drones in law enforcement has had a positive impact on the outcomes of police operations. Over 347 USA government departments use drones, with a growth of 518% in their use (Margaritoff, 2017).

### 7.3.3.3 Controversies Surrounding Security Robots

Robots have not only been used in providing security services in buildings but are also being used in carrying out military work. Air Force pilots in Syracuse, New York, fire missiles from Reaper drones flying in the Afghanistan skies (Joh, 2017). The developers of military robotics have been looking at expanding their territory and selling their equipment to the police force (Joh, 2017) and it seems that this has materialised. In Dallas, a bomb robot was sent to kill the suspect of a tragic shooting that left five police officers dead and seven others injured (Joh, 2017). Connecticut police have also made a call to use drones with deadly weapons (Gilberstein, 2017).

The death of an alleged shooter in Dallas sparked much discussion on the reinvention of the spring gun that over the years has gained much disapproval. A spring gun is a gun rigged to fire when a string or other triggering device is tripped by a significant amount of force. It may not seem fair to compare a robot to a spring gun that lacks the subjectivity and judgement of an actual person (Security Distribution and Market, 2016). An armed autonomous security robot as part of its design has killed no one. However, police have used a remote-controlled robot to kill (Joh, 2017). This may be true but at the rate at which technological advancements are unfolding and creators of robots pushing for fully autonomous robots, robots will be operating on themselves without the assistance of humans. The symbiotic autonomy relationship which Gonzalez (2017) describes as a relationship in which robots recognise their limitations and ask for human assistance will be non-existent.

The big debate around these autonomous robots being developed is who would be held responsible for the death or injury of someone caused by a robot? Robots are programmed

with algorithms to function and to execute a certain function in certain situations in a certain manner. Moreover, with companies not being legally obligated to share trade secrets, it cannot be established if the algorithm used by a robot might be reliable in its ability to assess threats, or equally troubling, produce results with noticeable racial biases (Joh, 2017). Some designers of military equipment have addressed this problem by having a human “in the loop” to prevent killer robots that may try to kill on their own (Joh, 2017). Even with the human “in the loop”, the accuracy of the analysis of the situation cannot be confirmed. It is unfair to make a person decide or refute the decision made by a robot on something it analysed using algorithms (Joh, 2017). A robot does not have the intellectual capability of a person to analyse a situation and come up with different ways to deal with it. A robot can only deal with a situation in one manner through its programming of algorithms. A situation that the robot deems dangerous may not be as deadly as the robot perceives it.

There is already an agreement that was established between K3 robots and K5 Knightscope that made it immediately possible for customers in northern California to buy their robots with the option to purchase becoming available in southern California at a later stage (Security Distributing and Market, 2016). This was after the fatal incident in Dallas that happened, which is mentioned in the above text. With security robots already being sold to the public, it cannot be guaranteed that these robots will solely be used to provide security services.

There is much controversy around the use of drones because of their effect on the issue of privacy (Rice, 2019). Some people felt that drones militarised the spaces that they live in and that made it very uncomfortable for them (Rice, 2019). In South Africa, the South African Civil Aviation Authority (SACAA) Remotely Piloted Aircraft System (RPAS) Part 101 Regulations regulate the use of drones (The Outdoor Team, 2017). A study that was done in South Africa on market expectations focusing on safety and security drones shows that the rising awareness of integrating drones into existing security systems and services to provide actionable intelligence will lead to explosive growth (Slater, 2018). The study also revealed that there are developments for more specialised analytic software and capabilities that enable drone systems to gather crucial data for safety and security applications quicker and more efficiently (Slater, 2018). Drones with guns have now been developed, thus sparking the interest of several military forces (Russon, 2017). A prototype of this machine gun drone was made in 2012 in Russia. Duke Robotics, an American owned company, developed and unveiled the Tikade drone in 2017. The drone is armed with a machine gun and a grenade launcher able to aim and fire at enemies while flying in mid-air (Russon, 2017).

Unlike other countries, South Africa is still developing programmed drones, which could potentially propel security service providers to buy AI-enabled drones from other countries. Whilst AI technology is beneficial, it also has its risks and the advanced developments made

with the creation of drones are a cause for concern as some of them threaten humanity. A suggestion has been made that there be a global ethical response to AI. Esposito, Tse, Entsminger and Jean (2019) state that there needs to be an international body that will set the standards according to which moral and ethical dilemmas are resolved (Esposito *et al.*, 2019). This is taking into consideration that between countries there are different cultural contexts, policymakers and businesses (Esposito *et al.*, 2019), and what is applicable for one country may not apply to another. Moreover, AI applications do not tolerate ambiguity meaning that firms, governments, and other providers will need to make explicit choices when coding response protocols for varying situations (Esposito *et al.*, 2019). This may prevent the programming of algorithms in robots that are biased and thus allow for transparency within the development of security robots.

#### **7.4 Regulating the 4IR Technology within the Private Security Industry**

Policy and legislation are very pivotal for regulation. This is because they tell a story of what you believe in as a country and/or entity. One of the biggest concerns with the 4IR is that organisations might not be able to adapt, and the government might not be able to employ and regulate new technologies to capture their benefits (Shwab, 2016). In Britain, a White Paper on the regulation of 4IR technology was published in 2019. The White Paper established a Regulatory Horizons Council which aims to identify the implications of technological innovation and advise the government on regulatory reform needed to support its rapid and safe introduction (Secretary of State for Business, Energy and Industrial Strategy, 2019). To capture the benefits of the 4IR, Britain's 4IR White Paper states that there is a need to reshape their regulatory approach so that it supports and stimulates innovation that benefits citizens and the economy (Secretary of State for Business, Energy and Industrial Strategy, 2019). The need for reform is urgent as 92% of businesses from a range of sectors think they will feel a negative impact if regulators do not evolve to keep pace with disruptive change in the next two to three years (Secretary of State for Business, Energy and Industrial Strategy, 2019).

In South Africa, the Presidential Commission on the 4IR was established by the Minister of Communications and Digital Technologies in 2019. In 2020, a report by the Presidential Commission was published and proposed the country's overarching strategy for the 4IR as well as recommendations regarding the institutional frameworks and roles of various sectors of society within the broad plan (Department of Communications and Digital Technologies, 2020). The report looks at various sectors that the Presidential Commission believes will be impacted by the 4IR and that need to be developed for the country's economy to develop from them. One of these sectors includes cyber security, which is beyond the scope of this study. In respect to the physical aspect of private security, the report does state that

there will be an initial displacement of jobs and a transition period in which government, business and labour need to urgently prioritise re-skilling the current labour force for the future of work.

PSiRA's mandate includes promoting the development of security services and ensuring compliance with existing legislation by security service providers (PSiR Act, 2001). From the above text, it is evident that the private security industry needs to develop new security officer roles to curb job losses. The creation of new roles is demand-driven. In respect to existing legislation, the Protection of Personal Information Act No. 4 of 2013 (POPI Act, 2013) and section 101 of the Civil Aviation Regulations, 2011 are legislations private security industry must align with.

Due to the fast pace of growth of technology within the 4IR, there are concerns as to whether the current regulatory mechanisms and legislations will be able to be effective. A study by the National Gambling Board of South Africa (NGBSA) (2020), which looked at the impact of the 4IR on the current and future regulation of gambling in South Africa, makes the following recommendation:

“In response to the regulatory challenges posed by the 4IR and related technologies, various new regulatory approaches are being discussed and trialed at the global level. These include promoting agile governance and regulation which can more swiftly and effectively respond to regulatory concerns associated with new emerging technologies. Agile regulatory measures include developing regulations and codes under statutory law which tend to be promulgated far quicker and are easier to amend. Other responses include the promotion of co- and self- regulatory models which place soft law or principle-based obligations on business actors to ensure transparency and accountability in their use of technology”.

Seanego (2018, p10) argues that “the rapid pace of change and broad impacts, legislators and regulators are being challenged to an unprecedented degree and for the most part are proving unable to cope. Therefore, PSiRA's challenges of developing regulations that will regulate the ever-changing technological security equipment are not unique in the realm of regulation”. Seanego (2018) recommended that the PSiR Act, 2001 be amended and that the amendment Act must identify other types of security equipment not contemplated in section 1 of the Interception and Monitoring Prohibition Act, 1992 as amended that must be regulated. Concerns of discrimination, infringement of privacy and threats to humanity by security equipment will remain an issue if current PSiRA regulations relating to security equipment are not amended. This is partly because much of the regulated security equipment is imported from other countries and the algorithms of this equipment are unknown.

#### 7.4.1 The Impact of 4IR Technology on the Regulatory Mechanisms

The use of 4IR technology in regulating different industries still needs to be researched further. The NGB identifies 4IR technology as a digital monitoring tool that can be used to track activities in the gambling industry. This includes the use of AI for data analytics that can be used for policy decision-making. Xulu (2020) on the regulation of in-house security recommended that PSiRA's IT unit should create an application software (App) that will enable inspectors to see uninspected companies. Xulu (2020) further recommends that changes made on the registration system would automatically reflect on the Authority's database. This will enable potential employers to see if security officers are compliant with the Authority or not when checking their registration status on PSiRA's App. This study will also look at how PSiRA could advance the regulation of the private security industry of South Africa.



## 8. Research Findings

The following section presents the findings of the study, which are structured along with identified themes.

### 8.1 Challenges and Opportunities of the 4IR

#### 8.1.1 The Negatives

The 4IR is most probably the fastest-paced IR to ever exist. Already, there are First World countries that are believed to be now in the 5IR. When looking at the challenges that the 4IR has brought, many of these problems emanate mainly from the lag in technology that we are experiencing. This lag is also evident in the private security industry. Smaller security companies are falling behind in advancing themselves and including these new technologies in their operations. On the other hand, the bigger companies can afford the technology and include it in their operations. This poses a challenge to smaller private security companies in industries. Caluza (2020) and the consumer survey highlighted that one of the reasons why consumers employ certain security companies is because of the unique services that a security company can offer to their clients. There are participants that stated they would like to include more technologies in their operations to meet their clients' demands.

Another challenge that was identified in the findings is the lag in development, which the literature review highlights. Smaller companies were struggling with competing for work because they could not afford these new technologies that are in the industry. It was observed that as much as there is this technological revolution happening, most small companies were still in the First and Second Industrial Revolutions. Security companies with more financial muscle were already adopting the technology introduced by the 4IR. The exclusion of persons in the private security industry is no longer about being historically disadvantaged but it is now about being economically disadvantaged and excluded. This phenomenon was also evident in training schools. Currently, there is no PSiRA training on the usage of security equipment, however, some of the well-equipped training schools have started exposing trainees to the different types of security equipment. The trainees of these training centres have an advantage because they know how to use the equipment, which puts them in a better position of being employed when compared to a trainee of smaller training schools. Some of the participants reported that some security companies had already started retrenching their security officers and approaching security officers from other security companies who have been trained to use security equipment and provide CCTV monitoring. Instead of training their staff, security companies would rather retrench and approach security officers from other companies because training their officers would mean they would have to wait weeks for their officers to complete their training. This means that these security companies will lose money whilst their security officers go for training.



Some security company owners reported that they were reluctant to upskill their workers with the skills and knowledge on the security equipment and how to use them. One of the reasons that were stated is that most security breaches happen because of an inside job. Hence if the security officers were to understand how the equipment works, it would jeopardise the safety of the operations. Be that as it may, a level of trust is needed by employers to their employees, and technology is more traceable when compared to the traditional manner of doing things. Marc Benioff, founder of Salesforce, a cloud-based software company stated that business cannot be conducted in the 4IR without the trust of your employees, customers and partners (Regenesys Business School, 2020). Moreover, without trust, innovation is impossible (Davis and Mulcany, 2018). This means that businesses cannot leverage the investment made by implementing these new technologies in their operations.

Another concern that was highlighted by this study was the lack of openness by the security industry in adopting the new technologies brought about by the 4IR and the willingness to upgrade the way they conduct their operations. One participant stated that finances may be an issue preventing security companies from adopting the 4IR technology, however, security companies also short-change their security officers and businesses by not re-investing in them by upskilling their workers and providing technologies to their workers. Security companies get good contracts, but instead of investing in their security officers by advancing their skills and pay notch and exposing them to these new technologies, they would rather keep the money for themselves. Other participants stated that there were fears that the technology would lead to unemployment hence companies that work with security companies by providing the security equipment are sometimes met with resistance. They are only forced to work with these companies because it is something that the client wants.

The lack of acceptance of the technological changes brought by the 4IR is detrimental because the world is changing, and it will not wait for those who do not want to change. In his last speech, CEO of Nokia Stephan Elop is quoted to have said, "We didn't do anything wrong, but somehow, we lost". This speech was made in 2016 when Microsoft acquired Nokia. The lesson the industry can take from this is that if you do not change, you shall be removed from the competition. Nokia had not done anything wrong within their business operations, however, the world changed too fast for them, and they failed to change and adapt, and their competitors became more powerful, resulting in loss of business. This is the fate of many of the security companies that do not want to change and embrace the changes happening in the world.

### 8.1.2 The Positives

The 4IR may come with its challenges, however, it also comes with opportunities for growth and professionalising the private security industry which has been a call made by the industry for years. Through the 4IR, there have been advancements in security services within the private security industry which has led to the emergence of new vacancies within the private security industry, which will mitigate the job losses brought about by the 4IR. This statement is supported by Klaus Schwab (2018) who states that the 4IR is an advancement of the 3IR. One of these sectors is aerial security, which uses drones and helicopters to provide aerial surveillance when rendering security services. Moreover, aerial security offers safety to the security officers that work in remote areas. Instead of sending a person to attend to a scene, they can first send a drone and assess whether it is safe to send someone. Drones are also a deterrent to crime and it pushes crimes to other areas.

Drones and helicopters have been used in the private security industry as previously highlighted in the literature review, however, their use is more advanced and frequent when compared to the previous. Helicopters are now being used for cash-in-transit (CIT), accompanying the vehicles that are transporting the money. In the tracking sector, the use of helicopters is also prevalent with helicopters being dispatched when vehicles are stolen or hijacked, providing an aerial view for the response team on the ground. Helicopters are also used in anti-poaching when responding to a poaching incident and they sometimes form part of an armed response team.

Drones are also now being used in the CIT sector, providing aerial surveillance to armed response teams. The birds-eye view that the drones provide makes it possible for the drone pilot to spot danger from afar to alert the response team of any danger. Drones and robotics are also being used for 3D modelling, which is used to create security plans for buildings. These 3D models make it possible for service providers to identify any blind spots and prevent security breaches from occurring. Drones have also become more prevalent in the guarding sector, somewhat replicating aviation security but in residential areas. A participant in the drone industry stated that drone security is the same as aviation security, just as the perimeter or fence around the airport is secured, the same is done with drone security.

When comparing drone security to aviation security, it can be said that drones are used to secure the landside (which is the perimeter that is being guarded) to ensure that the airside (which are the homes and businesses premises) are safe. The use of drones in the guarding sector has to some degree led to job losses because with a drone you can half your staff complement. However, this also lies with the owner of the company as to whether they are willing to upskill their workers with the right skills for the drone to be used as a compliment to the work that they are doing instead of the drone being a substitute. It was

suggested that those security officers who are already working in the industry be upskilled and reskilled with the necessary skills to fly and work with drones and any other technology.

Irrespective of the fact that technology may seem to have the upper hand, humans are still very much necessary to work in the private security industry, especially in South Africa where there is a high crime rate. With the COVID-19 pandemic, many people lost their jobs, however, training centres reported that there was a huge influx of people who registered for PSiRA training when the industry was approved to conduct distance learning. One participant stated that the private security industry is COVID-19 resistant with people from professions such as engineering entering the industry so that they can get employment.

The 4IR has also seen an increase in the use of CCTVs, which have artificial intelligence (AI) and that use internet of things (IoT). Through IoT and AI, it has made it possible for security officers to render their services even when they are not in the vicinity manning the gates. Number plate and object recognition through AI has enabled boom gates to work on their own using automation. The automation process enabled by IoT makes it possible for the cameras to record and store data on servers and Cloud. IoT also makes it possible for end-users to monitor CCTVs on their phones. This has changed the face of control rooms in the industry.

CCTVs have also made it possible for the industry to professionalise and become more attractive for prospective security officers to work in the industry. The increased use of CCTV in the private security industry would mean that security officers would not have to walk for hours patrolling sites, they could monitor them from control rooms. It was mentioned that the Durban Municipality had plans to become a safer city with the focus being on the Durban Beach Front. Being a safer city would mean that a person's movements are captured by CCTV, making it possible to track them if they were to go missing. The biggest benefit of the CCTVs is that they act as a deterrence to crime and if security officers were to identify any suspicious activity in the control room, they could easily dispatch a response team to the area.

Just like the drone industry, CCTVs have created new employment opportunities. There are now people working in cyber services who protect the personal information that CCTV processes by using software. Others are creators of these software, which they install into servers that store the data. Others offer penetration testing to test the safety of their software. There are also mobile apps, security programs and software that are used using IoT, which security companies use for different security reasons such as access control and monitoring. These apps and programs have afforded security officers and people some sort of safety from contracting COVID-19 as they do not need to share pens when signing in for entry. These programs and apps have also made it cheaper for security companies to operate. It is no longer necessary for supervisors to drive to different sites. Security officers

can take videos and pictures of the places they are guarding and upload them together with the occurrence book. Some security companies use devices provided by manufacturers and distributors and some other companies use smartphones, which are a cheaper alternative.

There is a great improvement in the manufacturing sector. Seanego (2018, p.10) argues that “with the technology evolving at such a high speed, it is anticipated that the manufacturing of security equipment will continue to evolve as well”. The South African manufacturing space has infiltrated the international space with many of the manufacturers creating state-of-the-art access control equipment, which is exported to countries such as America and Germany. The drone industry is also prominent in the manufacturing space. One of the drone companies that participated in the study highlighted that they manufacture their drones locally. The hardware for these drones is sourced locally and the software is sourced in China. An invitation to participate in the study was extended to these companies, however, they stated that they did not believe that they needed to be regulated by PSiRA as they were not security guards or a security company, however, they did work closely with security companies.

The manufacturing space has been greatly neglected in terms of compliance and its regulation. Moreover, it is also another sector within the private security industry that has and continues to create new employment opportunities. The industry now has engineers and other professions in both the physical and digital space of manufacturing, which shows that the industry is growing. Moreover, the focal point of private security is no longer on physical security but the merging of the physical and digital space. PSiRA's Strategic Plan (2020) supports this statement by recognising the interconnectedness between security professionals and ICT professionals and the need to develop appropriate and cutting-edge standards and regulations.

## **8.2 Training in the 4IR**

### **8.2.1 PSiRA Grades**

One of the objectives of the Authority is to promote high levels of training as contemplated in section 3(f) of the PSIR Act, 2001. PSiRA has grades from A to E which security officers and business owners must undergo training for to be recognised as legitimate security officers. When the industry was asked about the relevance of the PSiRA grades in the 4IR, many of the participants stated that the grades were still applicable, however, they needed to be updated. One participant indicated that with some of the grades, there was a repetition of course content. It was also highlighted that the blanket approach PSiRA is using for the different sectors of the industry was not adding any value so much that other sectors did not see the need to even train and be registered with PSiRA. One of these

sectors are installations, which the PSiRA training does not cover. It was suggested that the PSiRA grades be the basic level training for guarding, which once completed can be complemented with additional training that is sector orientated.

### **8.2.2 The Blanket Approach of Training**

The blanket approach of training has made it difficult for security officers to perform their duties effectively. An example of this is drone security. It was reported that although security officers were PSiRA registered and had received the PSiRA training, they found it hard to work with drone pilots. A threat would be identified; however, it took security officers time to reach the location of the threat because they did not have any training on navigation.

Aerial security depends heavily on radio communication, which was reported that security officers could not do. The proposed PSiRA regulations for drones state that for a security officer to fly a drone, they need to have obtained a Grade C PSiRA training and have acquired their Remote Pilot License (RPL) from the SACAA. As it stands, the drone security industry is well underway developing its own training standards for drone security. This is because security officers with merely their RPL training find it hard to adapt to the security environment. PSiRA grades do not cover any of the geographical and meteorological aspects of flying a drone and will render irrelevant to the training of drone security officers. Drones are not merely drones, they must align with their purpose and so must the training.

The same sentiments were shared when it came to installations. Installers felt that they received no benefit from the PSiRA training as the focus of the training is on the guarding sector. Installation companies reiterated that they only registered with PSiRA because they wanted to be compliant. Security companies with installers trained their employees privately because there is currently no training on installation. One of the manufacturing companies of CCTV reported having been approached by one of the security companies to have their training material on installations accredited by SASSETA. In terms of the PSIR Act, 2001, the Authority is the only body mandated to regulate the training of security services. A SETA, on the other hand, as established by the Skills Development Act No. 97 of 1998 (SDA, 1998), is there to expand the knowledge and competencies of the labour force to improve productivity and employment. It was reported that SASSETA, as the relevant SETA of the private security industry, had skills training on installations, however, it was discontinued. Numerous attempts were made to get the participation of the SETA in this study to shed light on the reported training material on installation that they were formulating but unfortunately, those attempts did not materialise.

The industry highlighted their concerns on lack of training and regulation of CCTVs. The AI and IoT technology used for CCTVs makes it possible for security officers to be more efficient when working. Through AI, a missing person can be searched for on video footage

by the description of clothing they were wearing. IoT makes it possible for people to view live CCTV footage on a variety of devices. When not secured, IoT makes it easier for hackers to hack. And in this new digital era, it can be expected that crimes will be committed by using the very same technology meant to protect people. It was highlighted that not everyone is meant to be an installer because the technology in the 4IR is highly sensitive. Moreover, people who are installers must be ethical, and be fit and proper security officers. They also need to be knowledgeable and advise their customers on how they can protect their security equipment from being hacked. With an IP Address or MAC Address, a hacker can hack the live feed of a CCTV. It was suggested that PSiRA engage the industry or experts in the field of installation to create relevant course material that will look at the training, installation, selling and manufacturing of CCTV. Moreover, with the available technology, it was suggested that only a selected few should be allowed to use and install this technology. The PSiRA Strategic Plan 2020/21 - 2024/25 attests to this statement by stating that PSiRA needs to create a vetting capability to ensure that undesirables do not get involved in the industry.

### **8.2.3 Selling of Training Certificates**

One of the biggest concerns mentioned by the industry was the selling of training certificates by certain individuals. The selling of certificates has a very detrimental impact on the industry, resulting in untrained security officers entering the industry. Companies were reported to have spent hefty amounts of money in retraining security officers who have PSiRA certificates but could not perform their duties. One of the participants in the drone industry highlighted how chaotic it becomes when security officers have to communicate over the radio. Radio communication is one of the learning outcomes covered by the PSiRA grades. This goes to show that training certificates are indeed being sold.

The danger of the illegal acquisition of training certificates is that the industry becomes infiltrated by incompetent individuals. This not only tarnishes the image of the industry, but it also puts their lives in danger. The crime rate in South Africa makes the private security industry a lucrative business. However, with criminals becoming more brazen, security officers risk their lives every day when reporting for duty. This is not to say that all security officers that have died in the line of duty are not skilled, however, with appropriate training such as firearms training, they can be able to defend themselves.

Another detrimental issue that can be potentially caused by the selling of training certificates is having trainers who have not undergone training be trainers within the industry. The requirement to be a trainer is a PSiRA Grade E certificate and a minimum of one-years' experience and two-years' experience if working part-time. If a trainer happens to acquire their certificate illegally, it would be a cause for concern because this would typically mean that the blind is leading the blind.

One of the contributing factors to the selling of training certificates is that there is currently no assessment done to see if trainees have undergone training. One participant stated that the Authority should consider introducing an assessment in the form of an exam where it is written online in the form of a written assessment, which is something the Authority will be implementing. It was, however, highlighted that keeping everything online would give people the opportunity to cheat. It was then suggested that 90% of the assessment be done online and 10% done in the training centres where the training material was bought. This recommendation is partly feasible for urban areas as there is Wi-Fi and cell phone network coverage. In some small towns and rural areas, this would be not feasible in some areas as they do not have internet coverage let alone cell phone reception. Assessments are important despite this mentioned predicament. One proposed solution to this problem would be working with TVET colleges as many of these colleges are in many small towns and rural areas.

The private security industry has a significant impact on the growth of economies worldwide. In South Africa, it continues to grow because people are becoming richer and need their assets to be protected (PSiRA, 2020/2021). One participant mentioned that one of the reasons many people train to be security officers is because it is one of the jobs many people train for so that they can start putting food on the table after high school. This is true as the requirement to train as a security officer is to be 18 years of age. In terms of academic requirements for entry, none exist. This also makes it easy for individuals to buy training certificates because there are no indicators that raise questions as to how a person got entry into a training school and undergoing training. One participant stated that security work is considered to be bottom of the barrel work and the selling of certificates contributes greatly to this perception. Moreover, there is no practical training after attaining certificates. Security officers just go and work as security officers. A research thesis by Pillay (2020) on the growth and regulation of the private security industry in India and South Africa states that security work needs specialised professional training and universal recognition as an academic discipline.

A participant in the drone industry highlighted that the requirement to become a pilot for a remotely piloted aircraft is an age requirement of 18 years and above. However, they have noticed that people who are 18 years of age or above without a matric do not do well for their RPL. The training for a RPL costs thousands of Rands, hence a certain level of competency is needed for companies to not make a loss on training someone who will fail. This further highlights the importance of having an educational requirement for entry to train as a security officer.

## 8.2.4 Upskilling and Reskilling the Industry

Despite the fears that the 4IR is there to take away the livelihoods of many, the 4IR can create new employment if taken advantage of. One of the ways to do this is through the upskilling and reskilling of the industry and using the available talent pool.

The 4IR is bringing along a paradigm shift whereby security services are no longer merely about guarding but integrating technology in the rendering of services. The integration of technology in the rendering of security services is beneficial as it cancels out human error and assists security officers to work effectively. This paradigm shift calls for the upskilling and reskilling of the industry to stay abreast and relevant. The call for upskilling and reskilling is a call that all the participants highlighted as important.

The SDA, 1998 was established:

- “to provide an institutional framework to devise and implement national, sector and workplace strategies to develop and improve the skills of the South African work force;
- to integrate those strategies within the National Qualifications Framework contemplated in the South African Qualifications Authority Act, 1995;
- to provide for learnerships that lead to recognised occupational qualifications;
- to provide for the financing of skills development by means of a levy-grant scheme and a National Skills Fund;
- to provide for and regulate employment services; and
- to provide for matters connected therewith.”

One of the ways of achieving this is through section 9 of the SDA, 1998 which establishes SETAs. One of the functions of the SETAs is to allocate grants in the prescribed manner to employers. The grants by SASSETA were identified as one of the ways in which the industry can upskill and reskill its employees. The allocation of funds is done through the Workplace Skills Plan (WSP) whereby the employers identify scarce and critical skills by conducting research. The employers then identify a gap and can submit their application for the discretionary grant.

One of the challenges with the allocation of discretionary grants is that many people reported that although they apply for them they never receive the grants, and they are said to be given to certain security companies. One of the reasons could potentially be how the employers fail to articulate their need for funding. There is a possibility that employers need guidance in how to conduct research to identify scarce and critical skills. Another possibility



would be not knowing that they are supposed to register with SASSETA even though their payroll does not meet the threshold of R500 000. It is also not clear whether there is a rotational system in place to ensure that every security company gets an equal chance to be allocated funding.

PSiRA's training unit identified the absence of the Regulator in the allocation of grants as problematic. This is because the grant allocation is done by the judge and the jury. If the goal of upskilling and reskilling is ever to be realised, PSiRA and SASSETA need to work together to ensure that all employees and employers can access funding to address the issue of scarce and critical skills within the industry.

### **8.3 “TRANSFORMATION” in the Industry**

One of the detrimental factors of the 4IR is its financial constraints. As previously mentioned, the exclusion of people in the industry is no longer based on historical disadvantage but economic disadvantage as well. The majority of the participants of this study owned Small, Medium and Micro Enterprises (SMMEs) and most of them were historically disadvantaged. When asked on the topic of transformation, many stated that it needed to start by forging relationships between SMMEs and bigger companies. Participants highlighted how bigger companies could benefit from such partnerships. Theirs would be to bring their Black Economic Empowerment (BEE) status which would assist bigger companies in attaining tenders. This is not a new practice in the country. The National Building Regulator (NBR) is said to require big companies to subcontract 25% of contracts to Level 1 BEE companies, which they investigate to ensure that the owners are not merely a front but the actual owners of the business.

Unfortunately, in the private security industry, such mergers do not take place between SMMEs and bigger companies. The bigger companies forge relations with each other, making it difficult for smaller companies to bid for tenders. This is a practice that the Competition Act No 89 of 1998 forbids as it results in unequal and unfair chances of tender bidding. The transformation of private security is not only about redress, but also about creating opportunities for the entire industry through equal and fair economic participation (PSiRA, 2020/2021). The SMMEs reported that they used the PSiRA specifications, resulting in higher tender pricing. With the bigger companies, they would bid lower because they had the financial muscle. The security officers were said to be the ones bearing the brunt of this practice by being underpaid. It was suggested that PSiRA have a calculator on its website and app with all the fees, which is also currently being developed by the Authority.

Through the research, it also emerged that bigger security companies were “empowering” SMMEs by allowing them to use their company name at a certain percentage of their revenue. This practice is exploitative to some degree as these SMMEs were actually the

ones empowering these bigger security companies with their BEE status and paying them as well. Beneficial partnerships in the industry must be encouraged, however, when there is exploitation such practices need to be questioned when done in the name of transformation. Transformation is about a culture that advances equality, worthiness of humanity, ownership, and business and educational opportunities in the industry (PSiRA 2020/2021, p.22).

Given the increased interest of drones in the industry, drone companies were pushing for security companies to own their own drones instead of subcontracting drones from them. One hindering factor was the cost of a drone, which roughly costs R250 000. Then there is the Remotely Piloted Aircraft System Operating Certificate (ROC), which costs R400 000 for a company. Without a ROC, a business cannot own and operate a drone. A business model was suggested whereby small security companies buy and register their drones with bigger drone companies. When they can afford to have their own ROC, they then dissolve the partnership and become independent. This is a partnership that should be encouraged given that it benefits both parties and is within the confines of the law.

#### **8.4 Adopting Best Practices Locally and Internationally**

The report by the NGB highlights how the law falls short in regulating emerging and advanced technologies such as those of the 4IR because they often fall behind the pace at which these new technologies are developed. One way to overcome this hurdle would be by conducting impact assessments of new technologies before they are deployed in society. The Authority needs to apply this practice as it will ensure that the new technology is regulated and used within the confines of the law. One of the manufacturing companies that participated in this study stated that a large portion of the revenue is reinvested into their company for its research and development to create a product that is relevant for the people. The Authority needs to invest in its research and development and apply the findings and recommendations of the research to ensure effective regulation of the industry.

The Security Industry Authority (SIA), which is the regulator for private security in the United Kingdom (UK), has made it mandatory that security officers top up on their existing training to be able to work in the 4IR. This is a practice that the Authority can adopt as part of the upskilling and reskilling of security officers. These top-up modules must be developed and made mandatory so that security officers do not find themselves in the predicament of being retrenched because they do not have the relevant skills.

## **8.5 Regulating the Private Security Industry**

### **8.5.1 PSiRA Inspections - Using 4IR to Ensure Compliance**

One of the ways in which PSiRA enforces the PSIR Act, 2001 is through inspections. PSiRA inspections are divided into two sections. Firstly, there is the enforcement side of inspections whereby inspectors physically go to the site and investigate. Their investigations include taking pictures, statements and documentation from consumers and/or security businesses. The second portion of inspections is the compliance aspect. With compliance, the initial inspection is more educational where the security service provider is guided and educated and is more on the infrastructure inspection. The inspection then becomes more formal later. Inspectors then go there to investigate and insist on having certain documentation available. The educational approach is still there, inspectors still listen to questions and provide guidance, however, they will take action as provided for in PSiRA's law enforcement strategy.

The application of 4IR technology for inspections is more practical on the compliance aspect of inspections and can happen on an IT platform. This is because this type of inspection relies mostly on what the inspector is given by the service provider. Generally, an inspection is done by making an appointment to visit, then the inspector will request documentation, ask questions and complete a report. The inspector then populates the information and updates records. They then print and share the report then it is saved on the shared drive. The application of 4IR on the enforcement aspect will prove difficult, however, when the compliance raises concerns an enforcement inspector can then be deployed to investigate.

The envisioned approach would be using a system similar to e-Filing for a compliance inspection. Applying such an approach would be beneficial for the Authority and increase the number of inspections. A shortfall that was highlighted with Compiere is that some companies in rural areas were identified as being in urban areas. When inspectors would want to conduct inspections, it would prove hard to locate the businesses hence some businesses have had only one business inspection and that being the initial infrastructure inspection. The Strategic Plan 2020/21 - 2024-25 warns of the threat to the reputation of the Authority by the continued operation of non-compliant security officers in the industry.

#### **8.5.2 Security Equipment - To Regulate or Not to Regulate?**

The study by Seanego (2018) on the manufacturing, importation, selling and distribution of security equipment in South Africa highlights many legislative shortfalls the PSIR Act, 2001 has on the regulation of security equipment. In terms of the Act, it is only those involved in the installation, servicing and repairing of security equipment as defined by the PSIR Act, 2001 that is regulated by the Authority. Hence many of the manufacturers that were

approached in the study did not recognise PSiRA as their regulator because, legally, PSiRA has no jurisdiction despite them manufacturing, importing, distributing and advertising security equipment.

Seanego (2018) also highlights a shortfall in the regulation of manufacturing, importation, selling and distribution of security equipment. The PSIR Act, 2001 subject's regulation to monitoring devices contemplated in section 1 of the Interception and Monitoring Prohibition Act No. 127 of 1992. Those security service providers who perform duties of manufacturing, importation, selling and distribution of monitoring devices were also left in the dark as to why they should register with PSiRA because they dealt with software and not devices as stated by the Act. The software enabled the devices to function and not necessarily that they dealt with the devices.

When asked if PSiRA should regulate security equipment through inspections, different views were shared. One view shared was how would PSiRA accomplish such a task as security equipment is broad. A cell phone with a camera could be considered a security device. How could one inspect a cell phone and where would the line be drawn in terms of regulation? It was suggested that only the person using the security equipment be regulated and not the security equipment itself.

On the other hand, the industry and internal PSiRA staff believed that PSiRA should regulate security equipment. The technology that is used for security equipment is quite dangerous if it is in the hands of the wrong person and used improperly. Many of the security service providers use equipment to conduct their work. For example, private investigators (PI) will not just use their natural bodies to conduct their business, they also rely on devices such as recorders and bugging devices to intercept calls. For a PI to use a bugging device, they need to get a court order. If evidence is given to the investigating officer without the proper channels being used, the evidence would be considered null and void and the consumer would have paid for bad service. A PSiRA study by Netshivhuyu (2017) highlighted how the lack of regulation on the use of security equipment resulted in PI operating in a grey area. Private Investigators would sometimes give the devices to the consumer to plant to avoid any trouble in the future.

There also happens to be the POPI Act, 2013 and the Promotion of Access to Information Act No. 2 of 2000 (PAIA, 2000). These two pieces of legislation are probably one of the important Acts as they deal with the protection and processing of personal information. Security equipment used now needs to comply with these two Acts as almost if not all security equipment mentioned in the PSIR Act, 2001 and other security equipment not mentioned process personal information. And in terms of the POPI Act, 2013, security

service providers must oblige to the Act by protecting the personal information of people. Currently, in the industry, many companies are manufacturing security equipment. One device in particular that has grabbed the attention of many is the licence scanner, which is used upon entry in most places of business.

One of the concerns that were highlighted with security equipment was how it over-processed the personal information of individuals. Another worrying aspect is how these manufacturers acquire the personal information of individuals because as the licence is scanned, a picture and licence number of the individual driving filters through on the scanner. The PAIA Amendment Act 31 of 2019 states that the personal information of a person processed for a particular reason must never be shared with others; it is only processed for the consented reason and nothing else. South Africans have never consented to giving scanner manufacturers and companies their driver's licence information seemingly they have it. The question is 'how was the personal information of people in the country then acquired'? This is another reason why security equipment needs to be regulated as well as the people that manufacture, distribute, sell, import and advertise. The PSiRA strategic plan also supports this stance by stating that "PSiRA has to come up with rules that keep consumers safe while keeping pace with technologies. The Authority needs to regulate and provide clarity and predictability on the use of drones, apps and similar technologies of the future. This will require the regulation of both people and technology" (PSiRA 2020/2021, p.28).

The POPI Act, 2013 requires that the personal information of people be stored securely. All industries have been impacted by the POPI Act, 2013 as it is required by law that everyone abides by it. The private security industry is by no means exempt from the POPI Act, 2013. Hence the equipment used for the processing of personal information and its storage must be POPI compliant and must be registered with the Information Regulator South Africa (IRSA). The danger of not regulating security equipment is that the Authority will lose relevance to the industry. The industry is evolving and so must the regulator regulating the industry. As it stands, control rooms, which are part of the security services, that are subject to PSiRA inspections are being regulated by the industry. The danger of this is that the industry will self-regulate, security guards will decrease in the next coming years and the regulator will be left to regulate security guards alone.

The lack of regulation of security equipment will also mean that companies that manufacture, import, sell and distribute security equipment can open shop in the country and not be subjected to regulation. Many online shops and distributors are operating openly. Some of the security equipment is of inferior quality, which the public is sometimes not aware of. Hence the need to regulate and grade security equipment according to its superiority.

## 9. Recommendations

This part presents recommendations as informed by the data collected.

### 9.1 Security Equipment

When it comes to the regulation of security equipment, it is no longer a question of whether there is a necessity to regulate but a matter of it being a must. The Authority needs to implement the findings and recommendations made by Seanego (2018) relating to the regulation of security equipment as they are still applicable and relevant. Given that security equipment has also advanced, the research also recommends that security equipment used for purposes of aiding in the rendering of security services must:

- Undergo ethical hacking and receive certification that states that it is safe and secure to use. This recommendation applies to all security equipment that captures a person's personal information (e.g. images, ID number) as per the POPI Act, 2013. During inspections, the inspectors must check the validity of the certificates. If it is found that the certificate has expired and has not been renewed, the equipment must not be used until its firewalls have been upgraded.
- The Authority needs to grade security equipment that is manufactured, imported and distributed as suggested by the research participants. Consumers cannot be dictated as to which security equipment they must use; however, the Authority is mandated to protect the interests of the users of security services. Consumers will then be able to purchase security equipment knowing if it is inferior or the best product on the market.
- Inspectors can also check if the equipment is built to the standards of the South African Bureau of Standards (SABS) or any other international building standards. For radios used for alarms and armed response, they can check if they have the FSK number which is the frequency issued by ICASA, which is used to transmit alerts. This will ensure that there is no over-regulation and most importantly this will ensure that the equipment used is of the best quality and is used within the confines of the law.
- Part of the duties of PSiRA inspectors is to assist the industry and sometimes advise. It was recommended that more attention be given to regulating CCTV cameras. PSiRA inspectors need to be trained on the different types of CCTV cameras, their resolution and camera focus. During inspections, it must be established that the camera feed is secure, and the storage devices of the footage are also secure. PSiRA needs to set up standards for control rooms and service providers using CCTV cameras with IoT to have separate Wi-Fi connections to prevent hackers from hacking the live feed of the

cameras. Most importantly, inspections must ascertain that the CCTV cameras do not invade the privacy of the next person. If it so happens that the focus of the camera captures footage of a neighbouring building or home, permission must be given to the owner or user to have the camera recording in that position.

- The inspection of security equipment must be prioritised for public spaces such as business or office parks and shopping centres. A private individual can have their installed security equipment such as CCTV inspected on request.

## **9.2 Best Practices**

Research on technology needs to be conducted before it is deployed to society to ensure effective regulation. This means that PSiRA needs to invest more in its research and development and apply the recommendations and findings of the studies conducted.

The upskilling and reskilling of security officers need to be made mandatory and not for business owners to retrench staff because they do not have the technical skills. Just like SIA, PSiRA needs to have mandatory top-up skills training for security officers.

## **9.3 PSiRA Communication, Training and Registration Unit**

The Authority needs to prioritise creating relevant training course material for the training, installation, selling, distribution and manufacturing of security equipment. The Authority also needs to work with relevant stakeholders and the industry in formulating training material that is relevant and also affordable. The financial gap that the 4IR is creating needs to be addressed.

To prevent the selling of training certificates, a system whereby security officer trainees are to be assessed needs to be created. PSiRA certificates need to also have security features such as watermarks and unique QR codes assigned to individuals to prevent duplication and fraudulent selling of certificates. This assessment can be done online using electronic devices. The assessment can have anti-cheating software to prevent cheating and maintain integrity. It should also be expected that such an exercise will come with its challenges. It is not everyone that has network and Wi-Fi coverage. There is also the predicament of load shedding that the country experiences. The Authority can partner with certain training centres and have them function as examination/assessment centres. On the day that the assessments take place, training assessors can be deployed randomly to these examination/assessment centres to ensure that cheating does not take place. As a prerequisite to qualify as an examination/assessment centre, trainers need to be able to provide footage with a time and date stamp to ensure that cheating does not take place when assessments are done.

There is also a need to relook the requirements of entry in the industry for prospective trainers and trainees. It cannot be denied that many become security officers to be able to put food on the table. However, if the industry is to be taken seriously it also needs to have entry requirements besides age. It is recommended that the minimum requirement be a Grade 9. This is because persons in South Africa can enrol in TVET colleges for their National Certificate Vocational (NCV) or NATED National Diploma. The ability to read, write and converse in English is also required. Trainees need to be able to understand how the equipment is operated and that cannot be achieved without understanding.

This also applies to training instructors. A Grade E PSiRA certificate with one-year experience or two if working part-time is not sufficient to become a trainer. Trainers need to be also assessed to establish if they know what they are doing. Just like educators, they also need to undergo practical training and then be assessed. The argument by the industry has been that security officers are sometimes not academically gifted and having academic requirements will exclude those with learning difficulties. The industry can also look into having specialised training centres for trainees with learning difficulties and this also justifies the reason why trainers need to be trained and assessed.

In assisting the industry with staying abreast with the latest technology and training, the PSiRA Communication Department can organise webinars for the industry where they can be exposed to these technologies and skills development programmes. For those that cannot join the webinars, other video streaming platforms such as YouTube and even the PSiRA App can be used to upload the videos and be watched later. This will also help security companies build networks and assist in growing their security companies by venturing into other lucrative sectors. This is in line with the situational analysis of the PSiRA Strategic Plan 2020/21 - 2024/25. There is also a need to have a video created or circular sent to training schools or upload the previously mentioned on the PSiRA App on how to book. Many participants reiterated that many of their trainees and security officers were not able to make bookings because they did not know how to.

#### **9.4 Implementing Research Recommendations**

PSiRA is privileged to have a wealth of knowledge that has been attained by conducting research studies. The recommendations and findings of these studies, especially the report by Seanego (2018) on security equipment and its legislation and the training standards report by Gichanga (2016) are relevant and must be implemented. From these reports and other reports, templates for inspections on the different security sectors can be created and used when carrying out inspections. The other security sectors need not be neglected especially now at the time when there is a great technological change happening.



## 9.5 Mandatory Skills Development

The Authority needs to make skill development mandatory. Companies must not retrench their officers because they lack technical skills. This is inhumane, and it goes against the purpose of the SDA, 1998.

## 9.6 PSiRA Partnerships

It can be expected that much of the regulation of the industry will be of coexistence with other regulatory bodies. To ensure effective regulation, PSiRA will need to work with other stakeholders in fast-tracking the development of relevant training material and formulating relevant regulations.

# 10. Conclusion

Without a doubt, the 4IR is unfolding around the globe and impacting and affecting all the industries in the world. The private security industry is by no means immune to the changes brought about by the 4IR. Thus, this study was conducted to investigate the impact of the 4IR on South Africa's private security industry. This study aimed to explore the challenges and opportunities being brought by the 4IR to the private security industry, to explore the relevance of the PSIR Act, 2001 towards the 4IR, to explore the best practices in regulating 4IR technology in the private security industry, to discover the required training standards for the use of 4IR technology in the industry, and to determine which technologies PSiRA can utilise in regulating the industry.

The findings of the study highlighted some shortcomings in the PSIR Act, 2001, which could be detrimental to the regulation of the industry in the 4IR. The 4IR is changing the face of the private security industry either for the worst or the best depending on whether or not the opportunities it brings are utilised for the advantage of the industry. Job losses are to be expected, however, through upskilling and reskilling of the industry and the continuous identification of jobs created by the 4IR many people can keep their jobs and others be employed.

The study has made recommendations on how to mitigate the negatives of the 4IR. The recommendations also highlight how legislation needs to be amended to assist the Authority in effectively regulating the industry and how partnerships between regulators and the industry play an important role in regulation.



# 11. References

## Books And Reports

Caluza, L. (2020). *Defending the defenceless: A study on the regulation of anti-poaching as a security service in South Africa*. South Africa: PSIRA.

Cresswell, J. W. (Ed.), (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). Los Angeles: Sage.

Goodman, L.A. (1961). *Snowball sampling. The annals of mathematical statistics*, pp.148-170.

Kothari, C.R. (2004). *Research Methodology: Methods and techniques. New Age International*.

Durkheim, K, Painter, D and Terre Blanche, M. (2017). *Research in Practice Methods for the social sciences*. 2nd edition, Cape Town: UCT Press.

Dobre, V. (2017). *Internet of Things: Challenges and Opportunities for Private Security Perspective*. Oulu University of Applied Sciences.

Khan, S. S. and Khan, A, S. (2017). 'A Brief Survey on Robotics', *International Journal of Computer Science and Mobile Computing*, Vol. 6, No. 9, pp. 38-45.

Joh, E. E. (2017). *Private security robots, artificial intelligence, and deadly force*. University of California, Davis.

Seanego, T. (2018). *Conducting Business In A Grey Area: The manufacturing, importation, selling and distribution of security equipment in South Africa*. South Africa: PSIRA.

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.

Tongco, M.D.C. (2007). *Purposive sampling as a tool for informant selection. Ethnobotany Research and applications*, 5, pp.147-158.

Xulu, H. (2020). *Narrowing the gap: The regulation of in-house security in South Africa*. South Africa: PSIRA

## Websites

Algorithm, (n.d.) *Tech Terms Computer Dictionary*. Available at: <https://techterms.com/definition/algorithm> (Accessed: 1 July 2021).

Bebbington, S. (2014). *What is programming?* Available at: <https://yearofcodes.tumblr.com/what-is-programming> (Accessed: 1 July 2021).

Buckley, I. (2019). *What Is Coding and How Does It Work?* Available at: <https://www.makeuseof.com/tag/what-is-coding/> (Accessed: 2 July 2021).

Carter, J. (2019). The ReconaSense AI Platform for Physical Security. Available at: <https://www.reconasense.com/wp-content/uploads/Artificial-Intelligence-and-Physical-Security.pdf> (Accessed: 3 July 2021).

Cloudflare. (2021). What is the cloud? | Cloud definition. Available at: <https://www.cloudflare.com/learning/cloud/what-is-the-cloud/> (Accessed: 5 July 2021).

Coetzee, E. (2021). Security drones on patrol- don't get caught with your pants down. The Citizen. Available at: <https://citizen.co.za/business/business-news/2496369/security-drones-on-patrol-dont-get-caught-with-your-pants-down/> (Accessed: 3 July 2021).

Department of Communications and Digital Technologies. (2020). Report of the Presidential Commission on the 4th Industrial Revolution. Available at: <https://www.ellipsis.co.za/wp-content/uploads/2020/10/201023-Report-of-the-Presidential-Commission-on-the-Fourth-Industrial-Revolution.pdf> (Accessed: 10 July 2021).

Earls, A., Shea, S. and Wigmore, I. (n.d.). Definition: drone (unmanned aerial vehicle, UAV), Available at: <https://internetofthingsagenda.techtarget.com/definition/drone> (Accessed: 25 June 2021).

Esposito, M., Tse, T., Entsminger, J. and Jean, A. (2019). Why we need a global response to AI ethics? Available at: <https://www.weforum.org/agenda/2019/05/who-should-decide-how-algorithms-decide/> (Accessed: 30 June 2021).

Gilberstein, C. (2017). Connecticut police could get drones with deadly weapons. Available at: <https://www.thedrive.com/news/8844/connecticut-police-could-get-drones-with-deadly-weapons?iid=sr-link7> (Accessed: 29 June 2021).

Gonzalez, R. (2017). I spent the night with Yelp's robot security guard. Cobalt. Available at: <https://www.wired.com/story/i-spent-the-night-with-yelps-robot-security-guard-cobalt/> (Accessed: 1 July 2021).

Heath, N. (2020). What is AI? Everything you need to know about Artificial Intelligence. Available at: <https://www.zdnet.com/article/what-is-ai-everything-you-need-to-know-about-artificial-intelligence/> (Accessed: 1 July 2021)

Hill, A. O. (2017). What's the Difference Between Robotics and Artificial Intelligence? Available at: <https://blog.robotiq.com/whats-the-difference-between-robotics-and-artificial-intelligence> (Accessed: 1 July 2021).

IBM Cloud Learning. (2020). Artificial Intelligence. Available at: <https://www.ibm.com/za-en/cloud/learn/what-is-artificial-intelligence> (Accessed: 3 July 2021).

Johnson, M. (2019). 4 Ways Private Sector Security Professionals Can Make Peace With IoT Platforms Security Today. Available at: <https://securitytoday.com/Articles/2019/04/08/4-Ways-Private-Sector-Security-Professionals-Can-Make-Peace-With-IoT-Platforms.aspx?Page=1> (Accessed: 5 July 2021).

Lindsey, S. and Woolf, B. (2021). The new rules of security: How AI will transform video surveillance. Available at: <https://www.securitymagazine.com/articles/94961-the-new-rules-of-security-how-ai-will-transform-video-surveillance> (Accessed: 1 July 2021).

Margaritoff, M. (2017). Drones in law enforcement: How, where and when they're used. Available at: <https://www.thedrive.com/aerial/15092/drones-in-law-enforcement-how-where-and-when-theyre-used> (Accessed: 26 June 2021).

Mikell, G. (2014). Fundamentals of Modern Manufacturing: Materials, Processes, and Systems. United States of America: Wiley.

Mohammed, M., Khan, M.B. and Bashier, E.B.M. (2016). Machine learning: algorithms and applications. Crc Press.

Nanalyze. (2017). 7 Security robots "complementing" security guards. Available at: <https://www.nanalyze.com/2017/11/7-security-robots-complementing-security-guards/> (Accessed: 22 June 2021).

National Gambling Board of South Africa. (2020). Research To Determine The Potential Impact Of The Fourth Industrial Revolution On The Current And Future Regulation Of Gambling In South Africa. Available at: <https://www.ngb.org.za/SiteResources/documents/2020-21/Rsearch/Impact%20of%204IR%20on%20current%20and%20future%20gambling%20Final%20Comprehensive%20Report%202020.pdf> (Accessed: 10 July 2021).

Ndung'u, N. and Signé, L. (2020). The Fourth Industrial Revolution and digitization will transform Africa into a global powerhouse. Available at: <https://www.brookings.edu/research/the-fourth-industrial-revolution-and-digitization-will-transform-africa-into-a-global-powerhouse/> (Accessed: 20 May 2021).

Oxford English Dictionary. (2021). Robot, available at: <https://www.oxfordlearnersdictionaries.com/definition/english/robot?q=robots> (Accessed: 1 July 2021).

Rasheed, L. (2020). Our lives after the coronavirus pandemic. Available at: <https://www.aljazeera.com/news/2020/3/26/our-lives-after-the-coronavirus-pandemic> (Accessed: 22 May 2021).

Reinharz, S. (2019). Artificial intelligence poised to make great strides in security industry. Available at: <https://www.sourcesecurity.com/insights/artificial-intelligence-poised-great-strides-security-co-> (Accessed: 30 June 2021).

Rice, S. (2019). Eyes in the sky: The public has privacy concerns about drones. Available at: <https://www.forbes.com/sites/stephenrice/2019/02/04/eyes-in-the-sky-the-public-has-privacy-concerns-about-drones/#88c9d156984c> (Accessed: 29 June 2021).

SAS Insights. (2021). Internet of Things (IoT) - What is it and why it matters. Available at [https://www.sas.com/en\\_za/insights/big-data/internet-of-things.html](https://www.sas.com/en_za/insights/big-data/internet-of-things.html) (Accessed: 5 July 2021).

Security Distributing and Market. (2016). Universal protection service launches autonomous robot service. Available at: <http://content.ebscohost.com/ContentServer>.

Secretary of State for Business, Energy and Industrial Strategy. (2019). Regulation for the Fourth Industrial Revolution [White Paper] HM Government. Available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/807792/regulation-fourth-industrial-strategy-white-paper-web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/807792/regulation-fourth-industrial-strategy-white-paper-web.pdf) (Accessed: 10 July 2021).

The Outdoorphoto Team. (2017). What to know before flying your drone in South Africa (private use). Available at: <https://www.outdoorphoto.co.za/blog/what-to-know-before-flying-your-drone/> (Accessed: 1 July 2021).

Vu, C. (2018). Security aspects of the fourth Industrial Revolution. Available at <https://www.nst.com.my/opinion/columnists/2018/06/379465/security-aspects-fourth-industrial-revolution> (Accessed: 1 July 2021).

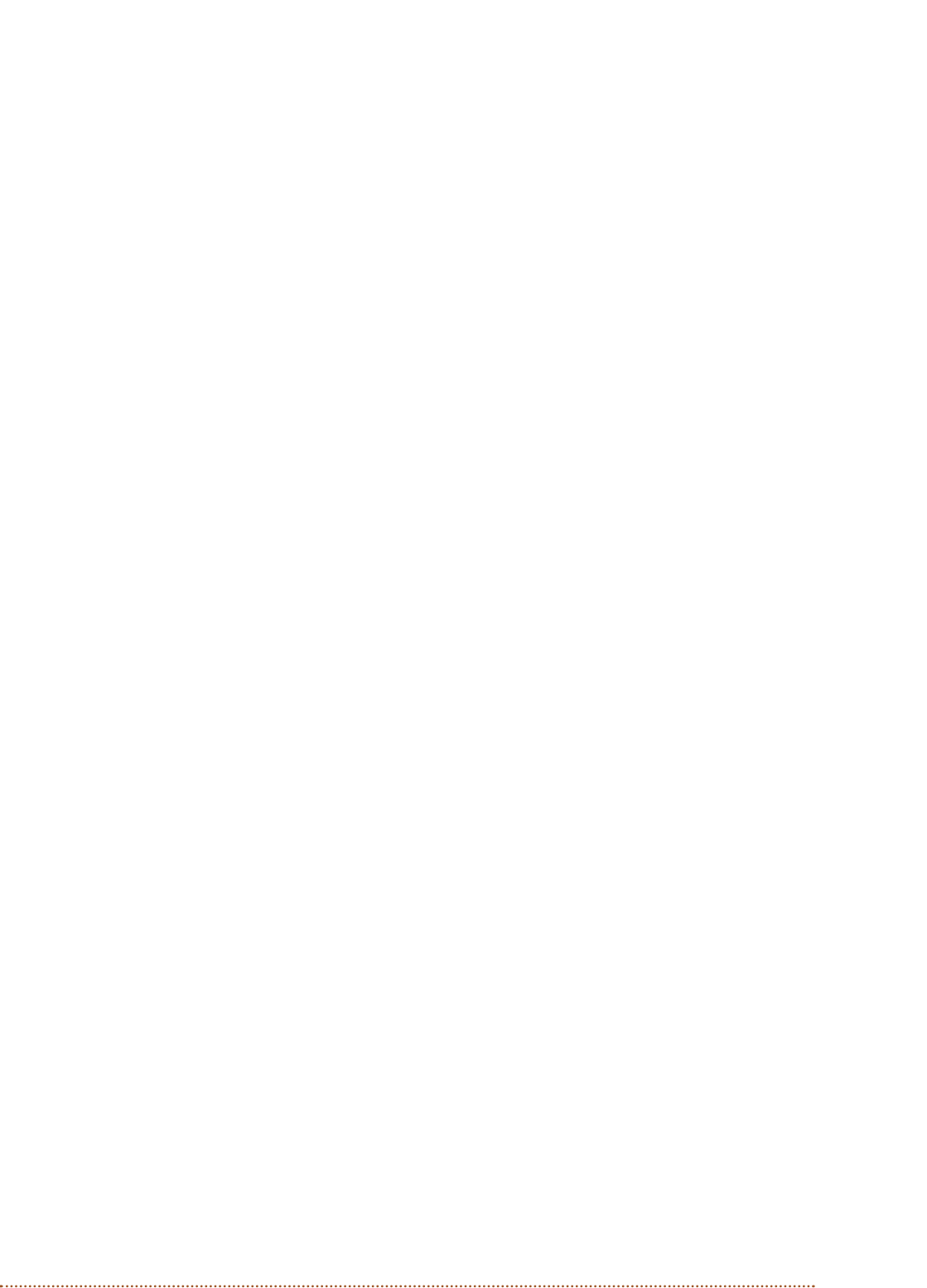
Williams, M. (2015). This Japanese security drone will chase down intruders. Available at: <https://www.pcworld.com/article/3013810/this-japanese-security-drone-will-chase-intruders.html> (Accessed: 25 June 2021).

## **Legislation**

Competition Act No 89 of 1998

Protection of Personal Information Act No. 4 of 2013

Promotion of Access to Information Act No. 2 of 2000

















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)

 082 803 4329

 Private Security Industry Regulatory Authority

 Psiralive