BACKUP SYSTEM TO THE GLOBAL POSITIONING SYSTEM AS A RISK MITIGATION FACTOR IN SOUTH AFRICA.

SOMANGAMANE BENJAMIN NTULI

STUDENT NO.9208912X

A research report submitted to the Faculty of Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management (in the field of Security)

13th June, 2014

ABSTRACT

Since South Africa's acceptance back into the international community in 1994, sanctions and disinvestments have ceased. Globalisation has introduced various technological systems such as the global positioning system (GPS) into the Republic of South Africa (RSA). Despite the many advantages of the GPS, it also poses certain threats such as linked services. A number of countries are engaged in finding a possible solution to this problem. As South Africa also uses the system, the purpose of the research study was to establish whether the country has a backup to mitigate risks to the GPS services.

To arrive at findings, a Critical Social Science (CSS) approach was applied. This approach led the researcher to use the Mixed Methods of Research. A case study was drawn from a sample of participants working in the defence and security environment. The study paid particular focus on South African constitutional imperatives with reference to the defence and security of the country from a national security policy viewpoint.

The researcher moved from an international to a national posture. He revisited the South African legal framework of national security policies and proceeded to locate the implications of the threats to GPS- linked services to South Africa and the African continent. These threats include selective availability, jammers, denial of service attacks and natural degradation.

The report confirms the existence of such threats and explains how other countries are dealing with them. The report also identifies additional challenges within the RSA and provides possible solutions to the vexing problem of GPS threats in the RSA.

DECLARATION

I declare that this report is my own, unaided work. It is submitted in fulfilment of the degree of Master of Management (in the field of security) at the University of the Witwatersrand, Johannesburg.

I further declare that it has not been submitted before for any degree or examination in any university.

SOMANGAMANE BENJAMIN NTULI

13th JUNE 2014

DEDICATION

I dedicate this piece of work to my late parents Momotho and Mthonyelwa, not forgetting my mother from the senior house, Dleni, my wife Sinah and our three children, Xolisile, Smangaliso and Noluthando, and Almighty God above all.

ACKNOWLEDGEMENT

The following people and institutions have been the cornerstone for my completion of the report and hence I express my gratitude to them.

My supervisor, Professor Anthoni van Nieuwkerk, for his guidance during this academic journey.

Professor Gavin Cawthra, for providing a broader orientation on security and development issues and the critical analysis thereof.

My syndicate members Bongi July, Phiroane Phala, Sonki Mothlabane and Thandi Mohale

Mr Kenny Makgathi for assistance with the review of the report.

Mr S M Ntuli for inspiration and motivation in execution of the report.

The Defence Research Institute of the South African National Defence and Belgium Campus IT-versity for supplying the resources to complete this work.

CONTENTS

ACRONYMS

AFREF	African Geodetic Reference Frame Project
ANC	African National Congress
ARMSCOR	Armaments Corporation of South Africa, Limited
AU	African Union
BRICS	Brazil, Russia, India, China and South Africa
CADSP	Common African Defence and Security Policy
CDMA	Code Division Multiple Access
CODESA	Convention for a Democratic South Africa
CNO	Computer Network Operations
e-LORAN	Electronic Long Range Aid to Navigation
EW	Electronic Warfare
GIS	Geographic Information System
GLONASS	Global Navigation Satellite System (Radio-based Satellite Navigation System)
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IBSA	India, Brazil, South Africa Dialogue Forum
ICT	Information and Communication Technology
IERS	International Earth Rotation and Reference System Service
IMF	International Monetary Fund
ISS	Information System Security
ITRF	International Terrestrial Reference Frame
ITRS	International Terrestrial Reference System
IW	Information Warfare
JSCD	Joint Standing Committee on Defence
LORAN	Long Range Aid to Navigation
MSDS	Military Skills Development System
MOU	Memorandum of Understanding
NCPF	National Cyber-security Policy Framework for South Africa
NEPAD	New Partnership for African Development
NGA	The United States National Geospatial-Intelligence Agency
NPC	National Planning Commission

NDP	National Development Plan
NDPC	National Development Planning Commission
PNT	Positioning Navigation and Timing System
PPP	Public Private Partnership
PSC	Peace and Security Council
RSA	Republic of South Africa
SA	South Africa
SAAI	South African Academy of Intelligence
SADF	South African Defence Force
SANDF	South African National Defence Force
SAPS	South African Police Service
SEA	Social Engineering Attack
SSA	State Security Agency
UAV	Unmanned Air Vehicle
WAAS	Wide Area Augmentation System
WGS84	World Geodetic System 1984
WTO	World Trade Organization

CHAPTER ONE: INTRODUCTION

1.1. INTRODUCTION

South Africa was freed from the shackles of apartheid in 1994 and has been democratically governed for the past 20 years. It was accepted back into the international arena with no more international sanctions and disinvestment (Jones, 2002). It behoves South Africa (SA) to embark on defence and security development projects, as much as on political, social, economic and other developmental fronts.

Words such as 'defence' and 'security' are carefully chosen. They are drawn from the broader conceptualisation of a development-friendly concept that embodies the individual, the government and society. The importance and relevance of this conceptualisation is informed by the historical materialism of SA and points to what is still required to extricate the RSA from the past, moving forward to a fully developed country.

To reconstruct the country, threats to national security must be identified. One of these threats is the Global Positioning System (GPS), which can be defined as follows:

> ***Global Positioning System (GPS):*** *A constellation of 24 satellites developed by the U.S. Defence Department that orbit the earth at an altitude of 20,000 kilometres. These satellites transmit signals that allow a GPS receiver anywhere on earth to calculate its own location. The global positioning system is used in navigation, mapping, surveying, and other applications where precise positioning is necessary (Kennedy, 2001; Leipnik, 2008).*

Although the system was established for military purposes in the United States of America (U S) in 1978, it has been so socialised that today it is also used in civilian life, in transportation, telecommunications, agriculture, mining, fisheries, and navigation to name a few (Pham, 2011).

According to Bartlett (2008), insurance companies use GPS to track vehicles and monitor vehicle mileage compliance with contractual agreements between the insurance companies and the vehicle owner or user. This is just one example of the benefit generated from the sound commercial application of a GPS.

Voigt, director of specialist CCTV and Space Television security equipment supplier, is impressed with the real-time tracking capability of the GPS. He is particularly impressed with the new Teltonika Hand Held Tracker, which he says has already proven itself overseas with its multiple real-time tracking capabilities suited to tracking employees, children, cars and pets. He explains how it works:

> *The device {is a combined} GSM (Global System for Mobile communication) and GPS (Global Positioning System) connectivity, which allows it to obtain device coordinates, then transfer them via GSM network. Owing to its small size, long lifetime, mobility and universal configuration, it's perfectly suited for applications where location acquirement of remote objects is needed as well as for securing company asserts. It can also track people, special events, and secret tasks and has been successfully used in search and rescue operations* (Voigt, 2009, p. 12.)

Voigt goes on to indicate that there is a Geo-Fence function "*which allows it to set restricted geographic areas and to send warning messages should an object cross the zone."* (Voigt, 2009, p. 14.)

However, this very useful and much relied-on tool has weaknesses that pose risks to GPS-linked services and subsequently to national security. The system is also sometimes abused in computer related scams such as cyber-crime. According to Ciampa (2010, p. 6.), 'car hacking' is done using GPS-linked devices that are able to demobilise car systems. Thieves operating a device make it impossible to lock car doors. Leaders in various fields need to be aware of these challenges/problems in order to provide guidance to the nation (Ciampa, 2010).

Technology changes rapidly and some of the weaknesses are undetectable until mishaps occur, hence the US government has put in place a professional team of expert executive engineers to monitor the capabilities of the GPS on a continuous basis. Russia, Japan and the United Kingdom are also investigating alternative backup mechanisms (Bartlett, 2008).

The backup system to the GPS is necessitated by the existence of possible jammers which pose a serious threat to the services provided by the GPS (Ruley, 2003). They are inexpensive

and readily available on the market. Whether by illegal acts or by accident, an intrusion poses a serious threat.

It is apparent that the research being undertaken focuses on the weaknesses of the GPS and GPS related technologies, and the implications that these weaknesses may have. As these weaknesses are an international phenomenon, SA needs to take note of them. The researcher intends to make recommendations to interested parties based on the findings of this study.

1.2. PROBLEM STATEMENT

It is unclear to the researcher whether SA has a mechanism in place to deal with the threats posed by the GPS. These threats include jammers, interference, aging degradation, intrusions, selective availability and cyber-warfare, which can all be detrimental to national security. The National State Security Agency, National Defence Force and South African Police Service need to be engaged in this matter as it falls squarely within their constitutional mandate and legislative framework to defend and protect the country and its people.

A formal research on GPS threats is therefore imperative if the objectives of national security are to be met. The aim is to provide the relevant authorities and general populace with vital information regarding challenges the GPS is facing and the implications that this has on national security.

1.3. PURPOSE STATEMENT

The purpose of this research is to investigate whether the RSA has a backup to the GPS. The question arises from the possible threats posed to the normal functioning of the GPS. How other countries mitigate these threats will also be investigated for there is a need to change this current situation.

1.4. RESEARCH QUESTIONS

1.4.1. Why does the Republic of South Africa not have a backup system to the GPS?

1.4.2. Is it possible for the Republic of South Africa to establish a backup system to counter the threats posed to the GPS?

1.4.3 What would the ideal system be for the RSA?

1.4.4. Is it feasible for the RSA to have its own independent stand-alone positioning, navigation and timing system (PNT)?

1.4.5. Will SA benefit by having a reliable GPS?

1.4.6. How can the RSA protect itself from challenges facing the GPS?

1.4.7. What intervention strategies are in place to mitigate the risks of the GPS in South Africa?

After having posed these questions, the researcher read broadly on the subject of positioning timing satellite systems (PNTs) and navigation systems, to gain more knowledge about the GPS and related systems. The aim is to find a possible solution for the South African situation in particular and other countries generally.

1.5 SIGNIFICANCE OF THE RESEARCH

1. To stimulate consciousness about the functioning of positioning, navigation and timing systems in general and the GPS in particular.
2. To draw the attention of the public and authorities to the strengths and challenges of PNT systems, including the GPS system. .
3. South Africa can invest in research and development to establish its own alternative and /or backup system to the GPS. The study will provide an opportunity for the improvement of the national security policy of South Africa.
4. Improvement of the national security policy may bring development to South Africa politically, economically and socially.
5. Although the research focusses on the SA situation, it is believed its outcome will be useful to any country to inform both private as well as public policy practitioners.
6. To link challenges faced by the GPS system to cyber-warfare and other security threats emanating from hi-tech crime.
7. To contribute to developing, strengthening and implementing the National Cyber-Security Policy Framework for South Africa (NCPF).

1.6 LIMITATIONS

Limitations included the cost to conduct the research but careful budgeting allowed this to be a mitigating factor.

Most of the participants were senior managers who cancelled appointments because of commitments. Some participants cancelled appointments while the researcher was on his way to meet with them. Because of continual cancellations, some participants had to be released from participating in the research. Others withdrew without giving reasons; the researcher respected their decisions, as their decision to participate was voluntary.

The books and other resources that provided information on cyber-security, cyber-warfare, cyber-terrorism and high-tech crimes were expensive. In addition, the researcher had to wait for more than 20 days for books ordered online from the Amazon bookshop, as these were unavailable at reputable SA bookstores such as Exclusive Books, van Schaik, Juta and Protea. There were further delays at Customs at the OR Tambo International Airport after the books arrived in SA.

To gain access to certain websites, the researcher was required to become a subscriber. This added to the cost of obtaining information.

As a part-time student, the researcher had to balance his time between his work and studies, and as a contractual employee, he had very little study leave.

Because of the sensitivity of the information, it had to be managed discreetly. The researcher had to maintain a sound rapport with the participants and take care not to offend other countries for fear of compromising diplomatic relations or SA's national security interests.

Whilst sufficient planning to undertake the research was in place, the researcher had to be mindful of ethical issues that could have a bearing on the success of the research (see below).

1.7 ETHICAL CONSIDIRATIONS

As the research dealt with information pertaining to national security, the researcher had to be cautious in managing information and its source. He had to take cognisance of applicable

protocols, e.g. seek permission to use the required information, inform participants of their right to withdraw from participation in the research study if they so wished. In addition, matters of security levels for vetting had to be adhered to because most of the interviewees were senior managers and professionals in their fields of work.

The researcher had to be conscious of problems relating to trust, confidentiality and abuse of information throughout the research process and beyond. These factors were mitigated by arranging prior meetings with the participants to build rapport and revealing that the researcher had received security clearance from the relevant RSA government institution. (Creswell, 2003, pp. 62–66).

The researcher shared how the study could benefit the participants in their field of work i.e. the mandate of the security sector (Fox, 2007).

1.8 SUMMARY

This chapter provides a background to the entire research report. It explains the problem identified, the purpose of the research study and the significance of the study. It poses questions the study is geared toward finding answers for them. It further highlights the limitations and ethical considerations. The next chapter will deal with the literature review. The opinions of certain scholars on the topic will be discussed in depth.

CHAPTER TWO: LITERATURE REVIEW

2.1 INTRODUCTION

In this chapter, the researcher engages with the literature of various scholars, authors and researchers about the GPS. The researcher explains how the GPS works, discusses its uses and identifies similar systems. The cost of these systems, the international and South African perspective, and the implications for developmental programmes for the African continent on GPS and also discussed. The chapter concludes with a discussion on the recorded risks associated with these systems.

2.2 HOW THE GPS WORKS

As already stated in the introduction, the GPS is an American technology that was initially designed to meet the needs of the military. Today its use has diversified to include fields other than the military. The GPS or the Global Navigation Satellite System is described as:

> *a constellation of 24 satellites developed by the U.S Defence Department that orbit the earth at an altitude of 20,000 kilometres. The satellites transmit signals that allow a GPS receiver anywhere on earth to calculate its own location. The global positioning system is used in navigation, mapping, surveying and other applications where precise positioning is necessary.* (Kennedy, 2001, p. 44; Leipnik, 2008, pp. 296–297).

Simply put, the GPS is a satellite navigation system that shows location and time anywhere on earth through linkage with satellites in space. For it to function optimally, it is linked to the Geographic Information System (GIS). GIS is a system designed to capture, store, manipulate, manage, analyse and present various type of geographical information. GIS is also known as an academic discipline dealing with geographical information. However there remains a clear distinction between GPS and GIS. GPS Triangulation is:

> *a method for figuring out a position using a calculation based on angles and lines between several satellites at different locations in space. The known locations of GPS satellites are used to in space to determine the distance between multiple satellites and your GPS receiver. From this data, the GPS uses calculations based*

on the geometric properties of triangles (hence the name triangulation) to determine your position (http://airandspace.esi.edu/gps/work.html)

A GIS system can be customised and its accuracy depends upon information stored. Such high level positional accuracy is usually provided by GPS-derived positions. GPS functionality and mobile devices is therefore increasingly integrated into GIS. Thus, it is essential to note that GPS is an important tool that GIS uses to establish positions and time. The two work together in complimentary to each other.

The GPS also uses other mechanical aspects such as ephemeris data which are divided into two namely, the ephemeris and almanac data. However, the discussion should surface without vouching into technical aspects.

2.2.1 World Geodetic System 1984(WGS84)

An important element that is fused into the GPS is the WGS84. WGS84 was developed by the US Department of Defence as a reference system involving global activities such as mapping, charting, positioning and navigation (Snay & Soler, 2000, p. 1). According to Snay and Soler (2001), the WGS84 is widely used for *'absolute positioning activities where people assume that satellite orbits are sufficiently accurate to serve as the sole source of control for positioning points of interest'*. The WGS84 is capacitated with both predicted and post-fit orbit reference systems. The predicted orbit reference system is based on calculations made in advance by using primary physical functions to induce the satellite's present locations. The post orbits use results from the preceding positions of the satellites. Post orbits are said to be more precise than the predicted orbits.

The WGS84 is said to be the datum used by the GPS. The datum is defined and maintained by the United States National Geospatial Intelligence Agency (NGA) and coordinates computed information from GPS receivers in terms of the WGS84 datum and the heights of the WGS84 ellipsoid. The technical description of the WGS84 datum can be obtained by clicking either on its website http.//geodesy.net/encompass/htm or on the NGA website.

Similarly:

> *the International Terrestrial Reference System (ITRS) is a world spatial reference system co-rotating with the Earth in its diurnal motion in space. The International Earth Rotation and Reference System (IERS) is in charge of providing global references to the astronomical, geodetic and geophysical communities and supervises the realization of the ITRS. Realizations of the ITRS are produced by the IERS ITRS Product Center (ITRS-PC) under the name International Terrestrial Reference Frames (ITRF). ITRF coordinates were obtained by combination of individual TRF solutions computed by IERS analysis centers using the observations of Space Geodesy techniques: GPS, VLBI, SLR, LLR and DORIS. They all use networks of stations located* on sites *covering the whole Earth*. (http://itrf.ensg.ign.fr/general.php)

Several realisations of the ITRF have been reported, the most recent being ITRF2008. The Hartebeesthoek 94 co-ordinate reference frame for South Africa is based on the ITRF91 (epoch 1994.0) co-ordinates of the Hartebeesthoek Radio Astronomy Observatory 36m antenna. The co-ordinates of TrgnNet stations, South Africa's network of continuously operating GNSS reference stations, are based on ITRF 2005 (epoch 2010.02).

Apart from the technical explanatory aspects, what is key to the study is the realisation that SA also contributed its part to its functional operations in the country, especially through the Hartebeesthoek 94. Therefore, SA should also pay careful attention to threats to the GPS, as these will have a bearing on us. This is further strengthened by relating to the Vertical Datum and the new South African Geoid.

The importance of the role played by SA regarding the expressed need for a reliable functional GPS is made by the NGI with the following statement:

> *The availability of the South African geoid model, described in detail in the article by Prof. Charles Merry and Garth Chandler (SaGeoid10.pdf), has marked an important milestone in the development of the geodetic infrastructure of South Africa which, in conjunction with the well established network of permanent GNSS base stations, TrigNet, has placed South Africa firmly at the forefront of geodetic science and its application in Africa. Apart from the over 50 000 well known trigonometrical*

> *beacons, town survey marks and bench marks, South African surveyors, engineers and geo-scientists now have the benefit of real time positioning services throughout the country and a high accuracy geoid model for height determination to give centimetre accuracy, three dimensional positioning, 24 hours a day.*

The above-cited strengths are the pillars SA could build on in addressing the challenges facing GPS. That the GPS is such a marvellous navigational tool is a compelling reason why its users in South Africa should know what the situation is regarding its potential threats. This research study, as outlined in the introduction, aims to contribute to the world's knowledge on the subject (Neuman, 2011, p. 124).

Geographic Information Systems (GIS)

The GIS is an information tool, a technological system loaded with geographic data. It is a

> *collection of computer hardware, software, and geographic data for capturing, storage, updating, manipulation, analysing, and displaying all forms of geographically referenced data.* (Leipnik, 2008, p. 296.)

Any potential threat to the GPS has the potential to affect the use of the GIS.

> *A future war and its outcome is likely to be based on strategic and tactical digital thrusts and defences across geographic boundaries where asserts are taken electronically, are remotely controlled, or destroyed by compromising their digital brains or storage medium. Communication technologies will become the means for massive digital attacks that compromise all matter of an adversary's command, control communications, operations, and stored information*. (Nugent & Janczewski, 2008, p. 31).

Clearly it is becoming increasingly important to consider the use of both the GPS and GIS.

There other critical issues pertaining to cyber knowledge that people in general and managers in particular, must know about, such as steganography, cryptography, IT critical infrastructure

and cyber terrorism, to name just a few. However, for now we need to pay special attention to the ethics of cyber war attacks, electronic surveillance and civil rights.

The main thrust of ethics in cyber war-attacks stems from international laws and conventions such as the Geneva Convention whereby even cyberwars are regulated so that their impact does not hurt or affect civilians and civilian installations.
This is not an easy matter to apply or even monitor. Countries who are signatories to these laws and protocols are expected to pass laws and align policies and practices to them (Rowe, 2008, pp. 108-109).

Electronic surveillance and civil / human rights is another necessary, albeit challenging aspect. Whereas cognisance is taken of the purpose of access cards / biometrics and cards to access social services such as pensions and government grants, their storage of information needs to be secured to avoid misuse. Electronic surveillance consideration also applies to the installation of surveillance cameras at places of work for instance, as these may interfere with civil liberties such as labour rights and the right to privacy. (Curran, 2008, pp.177-179)

As mentioned above, these two technologies can be deployed either simultaneously or separately depending on their purpose. Should the GPS experience difficulties causing risks to the services it dispenses, it could cause the GIS to malfunction as well.

People live in cyber-space i.e. an environment where satellites hang in the sky, are mounted or are launched from the ground. These include the 24 GPS constellations as well as those from other technologies such as the GIS and Internet, thus flooding cyber-space. Some of these technologies could be used to harm national security interests as will be explained below.

According to Neuman (2011), a literature review must:

1. *demonstrate a familiarity with a body of knowledge and establish credibility*
2. *show the path of prior research and how a current project is linked to it*
3. *integrate and summarise what is known in an area*
4. *learn from others and stimulate new ideas*. (2011, p. 124.)

2.3 DIFFERENT TYPES OF NAVIGATION SATELLITE SYSTEMS:

2.3.1 Global Navigation Satellite System (GLONASS)

The Global Navigation Satellite System (GLONASS) is a radio-based system developed by the former Soviet Union in 1976. It is operated by the Russian government through its Russian Space Force. It started with vigour but lost momentum due to a lack of funding as a result of the collapse of the Soviet Union around 1989. Currently, although Russia uses GLONASS, it is also joint venturing with China and India to strengthen their backup system to the GPS (Annual report to Congress: military and security developments involving the People's Republic of China, 2001:34-40). While Russia may also be secretly working on its own GLONASS, as these are sensitive security matters, suffice to say that GLONASS provides an alternative navigation satellite system to the GPS for the Russians.

The budget estimate is at 140.1 billion rubles ($4.7 billion) that were spent on the program 2001–2011, making it Roscosmos' largest project and consuming a third of its 2010 budget of 84.5 billion rubles. From 2012 to 2020 on, GLONASS from Russian budget allocated 320 billion rubles (10 billion USD).(Russia Beyond The Headlines. 7 December 2010. Retrieved 2011-10-06).

2.3.2 Galileo

Galileo is an independent global navigation satellite system currently developed and maintained by the European Union Space Agency as an alternative and complementary system to the GPS. It is named after the Italian astronomer, Galileo Galilei. Additional information about the system is that the European Union member states are collaborating in strengthening it for their mutual benefit, as it is expensive for each country to work solo to find solutions to threats posed to the GPS, including Galileo, in a common effort to tackle cyber-crime (Kilroy, 2008, pp.439-440). The project is said to be costing about €5 billion.

2.3.3. Compass

This is a Chinese independent satellite navigation system (the Beinou Satellite Navigation and Positioning Systems Project), launched in 2011 with 10 satellites. It was estimated to be in full operation with 35 satellites. In September 2003, China intended to join the European Galileo positioning system project and was to invest €230 million (USD296 million, GBP160 million) in Galileo over the next few years. (*BBC Business News*. 2003-09-19. Retrieved 2006-11-09).

According to an Annual Report to Congress of the People's Republic of China (2011), China is also collaborating with Russia, the US and India regarding improvements to the Global Navigation Satellite Systems. This is an interesting development regarding cooperation in research and development on military and security matters.

2.3.4. Indian Regional Navigational Satellite System (IRNSS)

The IRNSS is reported to be an independent regional satellite navigation system being developed by the Indian Space Research Organisation (ISRO). It is envisaged to be under the exclusive control of the Indian government. The reason for India to construct its own satellite system is similar to the one that motivated the researcher to conduct the study i.e. the possibility of selective availability of GPS services, which poses a threat to the national security of other countries.

> *The requirement of such a navigation system is driven by the fact that access to Global Navigation Satellite Systems, GPS, is not guaranteed in hostile situations. The IRNSS would provide two services, with the Standard Positioning Service open for civilian use and the Restricted Service, encrypted one, for authorised users (military). The total cost of the project is expected to be ₹1420 crore (US$217 million), with the cost of the ground segment being ₹ 300 crore (US$46 million) and each satellite costing ₹125 crore (US$19 million).*(NDTV. 2 July 2013. Retrieved 24 July 2013).

2.3.5. Long Range Navigation System (e-LORAN)

The LORAN, although of British origin, was re-established towards the end of the Second World War by the US Defence Department, thereafter it was upgraded to LORAN C and again it was upgraded to e-LORAN. Its purpose is to provide a backup satellite navigation system to the GPS as explained by the e-LORAN Technical Review Team. The essence of the matter is that moving from LORAN, to LORAN C, and now e-LORAN, this technological evolution has been and still is geared towards GPS backup, according to LORAN (2012, May 13).

e-LORAN has been left to decline and has almost been decommissioned. In order for it to be revived and operational again as an alternative backup to GPS, it is estimated to cost as follows:

If offset by an estimated $146 million decommissioning cost of existing Loran infrastructure, the IAT concluded that e-Loran could be established effectively for free. Going forward, e-Loran would require only the current $37 million per year in USCG operations and management base funds for Loran plus $20 million a year in new funds for five to eight years to complete all upgrades, new transmitters, and 'jump start' deferred maintenance.(http://www.insidegnss.com/node/1571)

The following are four significant factors worthy of note that have been summarily drawn from the above, as these will have a bearing on the research at some later stage during the data analysis:

1. A comparison of the various navigation satellite systems used or proposed by each country or region in case of EU.
2. The financial costs budgeted for each satellite system.
3. The collaboration or cooperation among regional states to join financial resources to fund their navigation satellite systems as they will also have implications concerning the nature of recommendations to be made at the end of the report.
4. The leadership role played by political leadership of various countries in leading similar programmes.

In summary, apart from the GPS, there are other satellite systems that are still being developed by some countries and some like GLONASS are being revived.

2.3.6. Other related technological systems

There are other clusters of satellite systems in the same environment, for example:

- *WAAS – Wide Area Augmentation System*
- *CDMA – Code Division Multiple Access*
- *Flex –system for synchronisation in a message* system.
- Electro- optical / infrared sensors
- Multi- mode radar synthetic aperture radar
- AIS-land –based and satellite
- Airborne- tethered aerostats, UAVs Aircraft manned- fixing helicopters

- Space- satellite- based sensors – imagery for vessels, oil pollution (deliberate / accidental) bathymetric space charts), weather, waves, currents, communications, etc.

The list is endless; however the point to make is an indication of a need for the RSA to broaden its scope of Research and Development to enhance development to bolster its own security, (Mokhele & Otto, 2011).

As can be observed from the myriad positions concerning navigation and timing satellite systems (PNTs) mentioned above, it is still not clear which ones belong to the RSA or not, which ones have a link or which ones do not have a link to GPS i.e. the GPS with risks already alluded to in the problem statement.

Some of the problems come as a result of economic trade among countries. This is partly the effect of globalisation. The term 'globalisation' is preferred in this instance, implying the movement of goods and/or technologies as a result of open trade among countries. Whilst the effect of globalisation impacts on almost every sphere of life, both positively and negatively, so do its dangers. Dangers are alluded to in a sense that free trade among countries also results in the moving around of technological equipment, without provision for solutions to their weaknesses and side effects or the skills to deal with them, leaving countries with the task of developing the required skills, lest they remain forever dependent on those who originated or sold them this equipment.

2.4 COSTS OF THE SATELLITE SYSTEMS

In discussing the different satellite systems above, cost estimates were given to inform the public and different governments to keep the financial costs in mind when considering a solution to the purpose statement of the report. The quotation below should help in brief:

> *Some of the factors that drive the cost of satellites are the equipment and materials used to build them. Running a satellite at a 36MHKz bandwidth will cost over 1.5 million a year. There are also the other gadgets and equipment that have to be built into the satellite in order for it to perform its intended function. These can include computers, computer software and cameras. Another factor that contributes to the expense associated with the satellites is the cost of putting one*

into orbit. It is estimated that a single satellite launch can range in cost from a low 50 million dollars to a high 400 million dollars. Launching a space shuttle mission can easily cost 500 million dollars, although one mission is capable of carrying multiple satellites and sending them into orbit. (www.globalcomsatphone.com/hughesnet/satellite accessed on 14 September 2013 9:03 pm)

The above information provides some indication of their willingness to find a backup or an alternative system.

The GPS is neither alone in this environment of navigation satellite systems nor immune to possible risks, there are also other related technologies that face potential risks. Therefore, the next discussion will be about the possible risks likely to befall navigation satellite systems and their use for other purposes either than those for which they were intended.

2.5 RISKS ASSOCIATED WITH GPS AND RELATED TECHNOLOGIES IN THE CONTEXT OF CYBER-SECURITY

In broad terms, cyber-security is an ever-present concern over safety and security matters. It is characterised by issues such as cyber-espionage, cyber-crime, cyber-warfare, hi-tech crime, cyber-stalking and spoofing. It is related to the GPS and the GIS regarding information management and operations, which is an important fact to be made about the trio in the security sector specifically and in life generally.

Technologically, there is a way whereby both the GIS and GPS capabilities can be combined to execute an objective. According to Leipnik*:*

digital cameras, GPS, and other sensors on Global Hawk and Predator unmanned airborne vehicle(drone) aircraft are transmitted to control centres outfitted with customised GIS programs that coordinate observation and occasionally direct attacks with Hell Fire missiles. A great deal of intelligence gathered from special operation troops, by CIA, and intelligence operatives is being built into GIS data sets, so GPS coordinates of suspected can be combined with aerial imagery and other layers to analyse, coordinate, and assess the

effectiveness of attacks often carried by stand-off aircraft which are themselves guided using GPS and GIS related technologies. (Monmonier, 2002 in Janczewski L. J & Colarik, A. M., 2008, p. 294).

There is an awareness that the GIS is not static, it is both expansionary and innovative. It is not static in the sense that newly acquired information can be loaded incrementally onto the existing information. It is innovative in the sense that the acquired information can be processed technologically, by increasing or decreasing the codification to attain the desired result. The combination of the GPS and GIS gives the former a better edge in the provision of services. Although this is explained in a simplistic manner, it should be abundantly clear that this is carried out by people with the necessary training and expertise. Engineering, geological, geographical, mapping skills and IT skills are essential to execute these tasks. However, it is equally important that policymakers have a reasonably good understanding of the basic operational requirements of such equipment, for they should be able to act more than just allocate the budget, they should be able to conduct oversight, monitoring, and the evaluation of applicable legislation and effect the necessary changes.

The next other linkage is cyber-warfare. Rowen (2011:41) explains Cyber-warfare as '*the use of exploits in cyberspace as a way to intentionally cause harm to people, assets, or economies'*. Like the GPS and GIS, cyber-warfare has become an issue in today's cyberspace. Cyberspace relates to the '*interconnected computers, servers, routers, switches and cables that make critical infrastructure network'.* (Rowen, 2011, p. 41).

Cyber-security has become another important concern, not only for SA but for the entire world. Its threats emanate from the violations of information systems, accessibility to private information and illegal access to banking information leading to the misuse of such data for unauthorised activities. This can be ascribed to the way technology has permeated every sphere of life today. It is largely manifested through the following:

a. *Cyber- espionage involving inter alia the silent gathering of information.*
b. *Cyber-crime involving inter alia malware, viruses, identity theft and attacks on financial institutions.*

c. *Cyber-warfare involving inter alia offensive information operations*." (*Defence Review*, 2012, p. 79)

Hence the inter-relatedness of the two technologies: the GPS and GIS in cyber-space where cyber-crime gets committed.

Terms such as cyber-warfare, cyber-defence or cyber-attack, are concepts used in the military environment as part of information warfare in the broader cyberspace. It brings in psychological defeat or victory depending on which side of the onslaught you stand. (*Defence Review*, 2012)

The need for backup measures as mitigation of the risks facing the GPS should be viewed broadly, as it also stands to mitigate weaknesses that may result from the misuse of the GIS in cyberspace as well. Further threats posed by cyber-warfare have been alluded to by various IT companies such McAfee, the ArcGIS Spatial Analyst, the Symantec antivirus software and security group, the Guardian Analytic, and the online banking security company. '*It is estimated that cybercrime cost about $110 Bn a year and affects roughly 1.5 Million people a day*' *(Business Day*, Wednesday, 20 February 2013:6-7). Hence, the importance of cyber-warfare in the same space as GPS and GIS should not be taken lightly.

Users of the GPS should be aware of the possible implications should relations with the US turn sour. If services continue to be threatened due to a lack of backup systems, the GIS will also be effected negatively.

A weak GPS and GIS will weaken the country's effort to counteract cyber-warfare. The country will be exposed to hostilities such as social engineering attacks, information warfare, cyber-attacks, spoofing and cyber-terrorism. Therefore, a re-look at the whole environment of information communication technology infrastructure and a call for a deliberate action on policymakers, leaders and managers to spare no effort to ensure management of cyber-space to minimise risks associated with cyber-warfare is critical.

As the research is conducted under a Course in Security Management, it makes sense that both security and defence policy frameworks are used as anchors for the work.

As life is not static, defence and the security of people and property require up-to-date systems for their protection. According to the constitutional mandate alluded to in chapter one, the Department of Defence (DoD) is to conduct a defence review to periodically re-assess the national security environment.

With reference to 16.1, 16.2 and 16.3, the researcher discerns that the DoD is looking forward to the type, calibre and capability of weaponry required to deliver on its mandate given the prevailing environment. It is in this light that the researcher raises the issue regarding the GPS in particular and the GIS in general in cyberspace. For it is their combination that produces significant changes to peoples' lives, either for better or worse .The quotation below informs us as to how SA regards these pertinent issues. SA should be commended for the establishment of a National Cyber-Security Framework:

> *to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information whilst strengthening shared human values and understanding of cyber–security in support of national security imperatives and the economy*. (*SA Defence Review*, 2012, p. 79)

It is within the above context that the commendable contribution of GPS, GIS, cyber-security and other technological systems are being appreciated. However, the researcher also underscores the weaknesses that lead to its abuse. This study expands the need to establish some means of backup to the GPS in order for both the people and the state to continue enjoying the services dispensed through these various technologies.

A new Defence Review Committee was established in 2010 with the following mandate and terms of reference that are relevant to the research topic:

> *The Minister of Defence further required the Defence Review to address the following key consideration:*
> *c. The strategic security environment, trends and predictions, and emerging sources of insecurity.*
> *d. The defence contribution to national security and an expression of South Africa's national interests."* (SA Defence Review, 2012, p. 43)

This highlights that the DoD needs to have an understanding of the security environment in which it operates and the trends and predictions of sources of insecurities in the national security interests. The research report is congruent with and complementary to government expectations. The report brings an added value in that issues of weaknesses and misgivings regarding GPS are investigated and analysed, and a solution is presented and hopefully implemented.

The commitment of the Ministry of Defence and the South African National Defence Force as a collective is illustrated by crafting and issuing a National Cyber-Security Policy Framework for South Africa calling upon the relevant defence and security clusters to provide their inputs. These are expressed under the executive summary contained in the Draft National Cyber-Security Policy Framework for South Africa.

The issue of *inter alia* cyber-security, information security governance and electronic warfare are all security concerns that should equally concern the national security interest stakeholders, be it electronic security or physical security.

2.5.1 Cyber-crime

When coming to challenges / problems faced by communication technologies in cyber-security, just as in GPS, there are threats that engulf cyber technologies. Cyber-crime encompasses '*any illegal act involving a computer and all activities done with criminal intent in cyber-space or which are computer-related*', (Kierkegaard, 2011, p. 438)

According to Kierkegaard, the growth of information and communication infrastructure leads to the socio-economic development of the country as well as providing opportunities for criminal activities. The above information is of critical importance for developmental states such as the RSA, for as the country improves economically, socially and politically, the potential threats alluded to earlier also increase. This situation also calls for developing states to address loopholes that may be exploited by cyber-criminals. Therefore measures such as the legislative and policy review are critical. We must embrace change even through our legislation and policies.

Kierkegaard mentions that amendments in the EU legislative include private offences such as the illegal collection of content-related offences, economic crimes and intellectual property offences. Kierkegaard adds:

> *as the European economy moves from a predominately industrial society to an information society, cyber-crime increases because most of the time criminals are ahead of government planning and good citizens see no need for immediate action as tomorrow is another day; criminals know that they must strike quickly and disappear before they are discovered while government will come later with a sluggish bureaucratic approach to dealing with these criminal actions. Governments and its employees must move away from this poor approach* (Kierkegaard, 2008, pp. 431-432)

Kierkegaard further identifies what she calls legislative and non-legislative matters. With the former, she refers to conventions, signed protocols, laws and policies passed through legislative bodies all geared towards curtailing cyber-crime. Thus the EU as a broader body ensures that member state countries ratify the protocols and pass related backup acts and policies.

Change to legislation is necessitated by the technological changes in the environment and a need to combat cyber-crime. This view was empathically put forward by the Council of Europe (CoE) in an effort to combat cyber-crime since 2000. This resulted in the listing of four categories of criminal offences in the CoE Cyber Convention, namely*:*

(1) *offenses against the confidentiality, integrity, and availability of computer data and systems;*
(2) *computer-related offenses; (3) content-related offenses; and (4) offenses related to infringements of copyright and related rights.* (Kierkegaard, 2008, p.433)

Kierkegaard further identifies non-legislative issues. These include what she refers to as 'contact points' to combat high-tech crime in which two major categories of threats are identified namely*:*

> *threats to computer infrastructure, which concern operations to disrupt, deny, degrade, or destroy information resident in computers and computer-networks, or the computer and networks themselves. … there are computer-assisted threats, which concern malicious activities, such as fraud, money laundering, child pornography, infringement to intellectual property rights, and drug trafficking, which are facilitated by the use of a computer.* (Kierkegaard, 2008, p. 436)

Because of the above issues, Kierkegaard is calling for the review of current legislation to amend these to close loopholes for any wrong doers. Furthermore, we should safeguard installations that may be targets for cyber-criminals such as the ICT infrastructure. SA and other countries can learn invaluable lessons from this EU approach to cyber-crime.

The point made here is that as cyber-crime knows no boundaries; countries need to cooperate locally, regionally and internationally to combat the scourge of cybercrime. Legislative appraisals must be conducted to close loopholes in the acts and policies to counter criminal conduct.

This takes us to a critical matter closely related to cyber-crime: information-warfare. As indicated earlier, the term was used mostly in the defence/security/military environment. However, because of the high incidence of computers and other technological communication systems today, previously privileged military information is now accessible to civilians and businesses. As expected, some of them do not have the knowledge on how to handle this information.

The term 'information-warfare' can be defined as:

> *actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary.* (Alger, 1996 in Janczewski & Colarik, 2008, p.25)

It is within the above context that security, cyber and information-warfare must be viewed as critically important aspects of national security as it has a bearing on the new paradigm of national security interests. Therefore, the security cluster and related stakeholders should pay

attention to these acts and policies in order to ward off cyber-war criminals. There are information-warfare trends that draw our attention to the environment in which we operate.

The following information is drawn from the work of Knapp and Boulton (2011, pp. 17-24):

1. *Computer-related security incidents are wide spread: this point refers to report surveys tracing numbers of attacks on public institutions as compared to the private sector. The results suggest that the latter is being attacked more than the former.*
2. *Entry barriers are low for cyber attackers: this means that cyber attackers find it comparatively easy to attack their target making use of technologies such as computers and the internet, to name but a few. The implication is that these entries need tightening.*
3. *Dangerous forms of cyber weapons have emerged; this comes with the history of computers- hackers too have shared information, combining their tactics so that they develop more dangerous ways to hack computers and internets.*
4. *Many nations have information-warfare capabilities: In the '90s, computers were not as popular as at present, for example in 2001 people in more than 30 countries were considered to be computer literate. Thus each country has devised its best strategic security plans based on computers. These can be attested to by looking at the military and security plans of countries like Beijing versus Taipei, Israel versus Palestine, Taiwan and Iran.*
5. *Increased economic dependence on information infrastructures: It is worth noting that societies have evolved, that is, from agrarian to industrial and now to information-based. In most organisations, whether governmental or private, computers as carriers of information, is basically non-negotiable.*
6. *The private sector is the primary target: At first government and military installations were the only targets, but now, since society uses ICT as well, it is increasingly being targeted.*
7. *Cyber-technology is increasingly used in corporate espionage: If you are in business you do not want to be less attractive to customers, you need innovation even if it may mean stealing information from your competitors strategically.*
8. *Cyber technology is increasingly used against individuals and small businesses:* Big corporate companies and governments have counter measures to protect themselves, but small entities and individuals are weaker and vulnerable to cyber-attacks.

9. *Cyber technology is increasingly used by organised crime: Organised* crime has found a safer and cheaper way of doing its business. If you want money find a way to either rob the banks, using IT or find entry into individuals' accounts.
10. *Cyber-technology is increasingly used against individuals and small businesses:* Simply put, it is less risky to steal from small organisations or individuals than from powerful entities, for these have more barriers to go through first. (Knapp & Boulton, 2011, pp. 17-24)

These are the trends that the Defence Review speaks about when it states the following on cyber security:

> *South Africa has established a National Cyber-Security Policy Framework whose purpose it is to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and understanding of cyber-security in support of national imperatives and the economy.* (*SA Defence Review*, 2010, p. 79)

These are further brought into the public domain by

> *this fearsome IT related problem follows the same military style modus operandi e.g. reconnaissance, penetration, then identify and expand the internal capabilities by paying attention to internal set up and increase access to more restricted areas, gain more knowledge about the internal environment, then inflict damage to the target. Hence, the importance of being aware of who one works with.* (Janczewski & Colarik, 2008, p. xv)

Janczewski abd Colarik (2008) also draw our attention to the CSI / FBI 2006 Computer Crime and Security Survey, which indicates that virus attacks are still the cause of major financial loses followed by unauthorised access, losses related to laptops and proprietary information. They indicate the following regarding the primary workings of cyber-attacks:

- *Virus and worm attacks that are delivered via email attachments, Webbrowser scripts, and vulnerability exploit engines*.
- *Denial of service attacks designed to prevent the use of public systems by legitimate users by overloading the normal mechanisms inherent in establishing and maintaining computer-to-computer connections.*
- *Web defacements of information sites that service governmental and commercial interests in order to spread disinformation, propaganda, and / or disrupt information flows.*
- *Unauthorised intrusions into systems that lead to theft of confidential and / or propriety information, the modification and / or corruption of data, and the inappropriate usage of a system for launching attacks on other systems.* (Janczewski & Colarik, 2008, p. xv)

These are critical patterns that we need to safeguard against in the IT infrastructure environment and computer usage generally. Both organisational as well as government plans should have room for implementation of the measures to manage the threats.

These information-warfare trends could be in excess of ten at the moment and are important messengers in all areas, including defence and corporate, to caution us about various kinds of attacks such as '*espionage, hi-tech espionage, organised crime, perception battles, and attacks from ordinary hackers or groups sponsored by nation-states or business competitors'.* (Knapp & Boulton, 2008, p.23).

GPS, as already explained, is a useful ingredient in the above-mentioned information communication technologies. Any issue that is likely to cause interference with its ability to perform should be of concern to its users whether directly or indirectly. Where possible, an alternative system should be sought to minimise the risks potential to any country's national security arrangements.

This is a necessary and appropriate security measure for countries such as South Africa who are on a developmental path where even small entrepreneurs and small enterprises need state protection. To this end, the SA government has economic incentives such as wage subsidies, farm schemes, start-up capital or key money that is offered as a once-off grant. There are also

tax concessions that starting businesses enjoy if they comply with the applicable legislation. All these constitute initiatives by the government to grow its economy in a developmental state. It stands to reason that there is a need to empower these companies so that they can grow economically and also withstand cyber-criminal attacks.

Another point to bring to the fore is the role of the Internet. According to Warren (2008) most societies use the Internet for activities such as communication and banking. Warren (2008) makes the following pertinent observation:

> *In many modern business environments, even the short-term, temporary interruption of Internet and e-mail connectivity can have a significantly disruptive effect, forcing people to revert to other forms of communication that are now viewed as less convenient. Imagine, then, the effect if the denial of services was over the long-term and also affected the IT infrastructure in general. Many governments are now coming to this realization.* (Warren, 2008, p. 42)

In light of the above, the following question is posed: are the developing states also aware of the concern, and if they are, what is being done to avoid such disruptions? These disruptions are part of the risks associated but not limited to technological systems, such as GPS, GIS and cyber technology, utilised in cyber terrorism, computer hacking, information-warfare and the like. These factors, therefore, should be considered by developing countries as priorities in their national security planning.

The South African Defence Minister made the following statement regarding cyber-security:

> *In terms of the national cyber-security effort, Defence will contribute to the national Cyber-Security Response Committee and Cyber-Security Centre. These structures will effectively coordinate departmental resources in the achievement of common cyber-security safety and security objectives.* (*SA Defence Review*, 2010, p. 213)

> *As GPS and e-Loran are originally American products, for them to be adapted to South Africa or elsewhere on the globe, intellectual property rights should be re-*

> *aligned with the recent view held in the economic world regarding the durability and applicability of such rights, and further inventions or improvements on them.* (Stiglitz, 2006, pp. 107-109).

2.5.2 Hi-tech crime

Related to cyber-warfare is Hi-Tech Crime. According to Knetzger and Muraski (2008, pp.52-53), Hi-Tech crime is described as crime that

> *involves e-mail harassment and threats, e-mail and Website scams, credit card fraud, identity theft, violation of restraining orders, child pornography (creation, possession, and redistribution), child enticement, hacking, drug trafficking, cellular / phone fraud, terrorism, and organized crime, and manufacturing fake identification.*

GPS plays a central role in the functionality of most if not all of this hi-tech equipment. Hence, it is necessary to have control over a satellite system such as the GPS. These crimes are committed with the use of computers, internets and the world-wide websites. According to Knetzger and Muraski (2008, pp.52-53), it is not easy to compile annual reports because most of these criminal activities are underworld dealings. Their impact on the economy, society and to some extent on politics is huge as it is a universal problem. Therefore, the initiatives by the South African Ministry for Social Development in inaugurating the Central Drug Authority (CDA) is spot on in dealing with Hi-Tech crime, coupled with the policy directive – the National Drug Master Plan 2013-2017 and complimentary work by the Inter-Ministerial Committee on Substance Abuse.(*City Press*, 24 March 2013, p. 27)

An intervention plan like the one of Social Development, is commendable. However, it should be backed up by the latest strategic views promulgated into acts and policy frameworks to combat cyber-crime. Other departments, not only Justice and Constitutional Development and the police, should assist with arrests and successful prosecution.

There is a need for an appropriate personnel-training programme to ensure properly trained staff execute tasks effectively, efficiently and diligently, for the computers used are the very same technological gadgets / systems that are used for GPS, GIS, cyber-space and information warfare in in th security and military environment.

The GPS constellations and GIS installation grids are also in the environment of cyber-space. These matters exacerbate environmental damage leading to global warming. This in turn affects the national security, as it affects climate change.

Climate change has become a debatable issue in the political, social and economic arena, resulting in the Kyoto protocols on emissions and the Doha protocols on trade issues discussed respectively. Although the researcher is not an expert in environmental issues, he wonders, as various satellites keep being launched in the sky, if and when they will be brought down and by whom? Who cleans these up after they have served their purpose or are they just being left there to possibly cause hazards even up there?

To illustrate how these issues have a bearing on national security, the researcher uses an issue that is currently debated in South Africa. Farm workers strike for better wages. Even before the onset of the strike, climatic patterns have been irregular: late seasonal rains, very hot or very cold conditions, water shortages and heavy storms. In short, pros and cons of these climatic changes belong to the Kyoto Summits. Kyoto protocols regarding global warming for instance, affect products for the market. Farmers no longer produce good products that reach the market in time, thus the market loses confidence in their products and starts buying less. Pricing and quota matters dominate discussions. All these are now under discussion as per the Doha agenda. The farm workers are unhappy because of wages that do not meet their expectations on the one hand, while on the other hand, farm owners are unhappy for they feel the workers are demanding unduly high increases. Production levels are affected, which has a ripple effect on production in the market.

In the above scenario, national security is threatened, especially when considering the stakeholders of the national security as alluded to in the Defence Review as well as the definition of national security as per the perspective of the new paradigm.

Thus in this context, all the different protocol discussions share a commonality: threats to GPS is critical because this technology is also used in agriculture e.g. watering sprays, tagging livestock, and timing-feeding for chickens. As these implementations are less labour-intensive

there are less production costs and more opportunities for high returns. However, they increase unemployment, especially of unskilled labourers.

The environment we live in today compels us to relate to other countries, be it on trade, military or security issues. In doing so, goods are moved from one country to the next. This applies to the GPS as a commodity as well. In this context, issues pertaining to patent rights and intellectual property rights arise under globalisation.

2.5.3 Cyber-warfare

Cyber warfare refers *to 'the use and exploits of cyberspace to intentionally cause harm to people, assets or economies'* (Rowe, 2008, p. 105)

Cyber-warfare operates in cyber-space. According to Libicki (2007), the term *'cyberspace'* was founded by William Gibson's 1984. Libicki explains cyberspace as follows:

> *Not only is cyberspace a construct, but rules of cyberspace are largely constructs - there is little hard-and-fast physics of sort that dictates what can or cannot be done say, in, outer space. What can and cannot be done in cyberspace need not follow the laws of physics or the laws of man – although violating the latter may have real-world repercussions.* (Libicki, 2007, p. 1)

Simply put, cyber-space is a man-made *'world'.* It can be a *'construct'* of constructed activities to accomplish a particular purpose using information communication technology. It is an essential security aspect that requires the attention of the public policy role players, and most importantly, members of the national security cluster. In the Draft National Cyber-security Policy Framework for South Africa, cyber-security is described as:

> *the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user asserts.* (Draft National Cyber-Security Policy Framework for South Africa, (2011,p.6)

The introduction and success of the Internet system has brought several successes. We can now advance their goal and destroy the purpose of the owners of the equipment. Libicki (2007) puts this as follows:

> *The real impetus is that the more cyberspace is critical to a nation's economy and defence, the more attractive to enemies is the prospect of crippling either or both via attacks on or through it.* (Libicki, 2007,p.1)

This means that as we use it, we should also bear in mind that we equally shoulder the responsibility to ensure that we do not lose control of this very important technology entirely.

The *UK White Paper on Defence* identifies similar challenges and cites cyber-space potential threats as following:

> *Cyberspace is complex, rapidly changing through interconnection and bringing us all closer together. This presents new opportunities and new challenges across the UK. The UK Cyber Security Strategy recently set out the approach we will take to realise the huge potential of cyber-space for the UK; making this country one of the most secure places in the world to do business in cyber-space, more resilient to cyber-attack and better able to protect our interest in cyber-space and help to shape and open vibrant and stable cyber-space which UK can use safely and that supports open societies.* (National Security Through Technology, 2012, p.10)

The above quotation provides an indication as to what extent some countries are prepared to equip themselves regarding cyber-space against cyber-crime.
Another critical point that has been made about technological challenges is one called high–tech crime. It cautions us against static security policies.

We need to change our technological security policies regularly in order to remain competent to deal with changes emanating from the forever-changing technological environment. This brings us to what is called the Third Law of Security: *'Security is a dynamic process. A small,*

continuously adapting security plan is much better than a large, static plan'. (Branigan, 2005, pp. 265-266)

Thus, in the ICT environment one must become accustomed to change – change in policies, operational codes, passwords and the like – and to minimizing undue access to ward off potential risks. While it makes our life easier, it also complicates it by introducing new ways of doing things and new risks. The California's High-Tech Advisory Committee's report cautions that '*we are implementing systems faster than we can secure them ... and we have no institutional memory. Earlier mistakes keep coming back to haunt us'.* (Branigan, 2005, p.358)

This indicates that cyber-security is an important matter in our discussion on the challenges attributed to the weaknesses of the GPS.

Recent newspaper reports mention that the theft of cars using technology to jam car remotes is on the rise. (Brenden Roane, p.6, *Pretoria News*, October, 2013.)

It has therefore becom more compelling for developing countries to find mechanisms to mitigate these threats. The lives of ordinary citizens and overseas visitors are continually being threatened. The costs to health and monetary values to individuals, society, companies, and state is immeasurable as a result. These incidents should inform the NCPF of SA. The draft National Cyber-security Policy Framework for South Africa states the following:

> 1.4 *The recurrence and growing incidence of cyber-attacks indicate the start of a new era in which the security of cyberspace acquires a global dimension and the protection of National critical information Infrastructure must be elevated, in terms of national security, on a par with traditional defence interests.* (NCPF, 2011, p.10)

Although legislations and policies are critical, the people and structures of civil society such as non-government organizations, community-based organizations, churches and other civil structures that are affected the most. Therefore, civil education remains of prime importance in creating an informed society to repel these social threats.

The CSI/FBI 2006 Computer Crime Security Survey on virus attacks and their impact on loses informed the public about issues we need to be aware of in the IT environment (Janczewski & Colarik, 2008, pp. xv-xvi)

The researcher is of the opinion that care should be taken when purchasing a product because quality, standards, environmental compatibility and the like are necessary for sustainability.

2.6 INTERNATIONAL PERSPECTIVE

The technological equipment used in both developed and developing countries may also be linked technologically to the GPS. Developed countries such as the US, Russia, United Kingdom, to mention but a few, are on record as stating that they are engaged in research and development to minimise the weaknesses of the GPS. However, the developing countries do not have research records in the same field of GPS, despite being consumers of its services. Any outage could leave developing countries in a serious dilemma.

The idea is not to instil fear among the developing countries or plant seeds of technological paranoia and remain sceptical towards the originators of this marvellous tool called GPS, but rather to bring some sense of legitimate concern that developing countries, too, need to have a backup system to GPS for any eventuality. They should also consider the establishment of an alternative system.

Perhaps developing countries are engaged in research to find ways to mitigate these GPS threats, but the researcher did not come across such initiatives. However, based on the literature review conducted thus far, the researcher is concerned that GPS threats might have a negative impact on the national security policy primarily of SA and its neighbouring states at a secondary level.

The brief highlights on the initiatives being taken by different countries regarding the positioning of navigation satellite systems serves as further exposure to SA and other developing states to the severity with which these matters are to be reviewed by them.

For example, the UK's White Paper on National Security Strategy, (National Security Through Technology, 2012, pp. 5-7) contains the mission to bring both the Ministry for Defence as well as the UK Armed Forces in line with their Future Force 2020. It covers the UK's new approach, open procurement, technological advantage, the UK Defence and Security Industry, government action and implementation plans to mention but a few. Their executive summary states the following:

> *Technology underpins most equipment and support arrangements. The global availability of technology combined with an ever-increasing pace of technological means that, in delivering the UK's defence and security, we face an increasingly capable and diverse range of threats. These are likely to include not only sophisticated military weapons, but also greater innovative and ingenious application of readily available civil technologies. Where adversaries can more easily buy high-technology products on the open market, this potentially reduces our operational advantages.* (National Security through Technology, 2012, p. 8)

The above quotation indicates the UK's commitment to take up its technological capability in line with current defence and security trends.

A preliminary conclusion can be made that indeed there are threats posed to the services of GPS and there are also alternative backup systems. Some countries, particularly the developed countries, have embarked upon research studies to address the challenges facing the GPS. The study is geared towards making inquiry as to why the RSA does not have a backup or an alternative system of its own. This leads to the next discussion focussing on the situation in the RSA.

2.7 SOUTH AFRICAN PERSPECTIVE

The RSA, like both the developed and the developing countries, uses GPS. The usage of GPS in the RSA should be viewed in the context of national security as conceived post-1994 taking into account the historic changes that have taken place. Keeping in mind that national security policy is shaped by various factors i.e. change in regimes, threat analysis outcome, a deliberate political decision a country may take and the like, it is necessary for the RSA to pay attention to the weaknesses that have been reported regarding the GPS in the interests of national

security. The White Paper on Defence of 1996 as well as the Defence Review of 2012 indicates that the RSA has done well in this regard so far.

However, flowing from these progressive policy directives, the question is to what extent do these policies address the challenges facing GPS in practical terms? This is the main concern of the study. The security factor is raised within the context of a new paradigm definition of national security that takes cognizance of all stakeholders, i.e. the state and human security. Before moving into further discussion, it is prudent that the laws and policies applicable in the RSA national security environment are briefly discussed.

2.7.1 Legislative framework

The establishment of security services in the RSA is directed by the Constitution of the Republic of South Africa, Act 108 of 1996. The Constitution (1996, pp.116–122) which provides governing principles as well as the outlining of establishments, structures and conduct of security services constitutes the defence force, the police service, and intelligence.

The South African National Defence Force (SANDF) is governed by the Defence Act 42 of 2002, the Defence Review and the White Paper on Defence of 1996. The National Intelligence, the South African Secret Service (SSA), and the South African National Academy of Intelligence (SANAI) are governed by the Intelligence Act no. 65 of 2002 and the South African Police Service (SAPS) is governed by the South African Police Service Act of 1999. These policy prescripts inform us where the security sector of the RSA draws its mandate and where the National Security Policy ought to be anchored.

2.7.2 Contextualising South African national security

A review of the national security policies as a whole are mirrored against constitutional mandates stated above, be it in broadly spoken about terms such as security transformation or reform. Any threats that may pose a challenge to any of the national security stakeholders (i.e. state or people) should be addressed accordingly, and threats emanating from the weaknesses of the GPS are some of the issues prevailing currently.

Thus national security policy should address these matters. Hence, the researcher's agreement with the view of public policy formulators and practitioners in the field of defence and security

in pointing out that national security issues are full of complexities. It includes factors to be taken into account in the best interest of both society and the state. These should be congruent with the national security policy, assuming that a national security policy already exists for the national security strategy has to be based on it.

Historically, the Convention for a Democratic South Africa (CODESA) introduced the pluralistic views of conceptual thinking about the new inclusive concept of national security. According to the *Oxford Advanced Learner's Dictionary*, CODESA is an abbreviation for 'Convention for a Democratic South Africa' that was a meeting of a group of politicians who discussed how South Africa would become a democracy. During the CODESA era, the ANC crafted a definition of national security and presented it through a document entitled 'Ready to Govern', which was adopted at its national conference in 1992 and presented at CODESA as follows:

> *the ANC identified lack of security in terms of underdevelopment, poverty, and an absence of democratic values as promoting conflict within and between states. Therefore, national and regional security should not be restricted to military, police and intelligence matters, but as having political, economic, social and environmental dimensions* (Hough & Du Plessis, 2007 in Cawthra *et al.* (2007, p. 17).

This new thinking had to find resonance in both the interim Constitution that was formally enacted and came into force in April 1994 as well as the current Constitution drawn up in 1994 and promulgated in 1996, marking the beginning of the new order. It drew a distinct separation between the old order and the new by bringing in new thoughts on the definition of national security in the context of the new SA. This was a very important year as a distinction was made between the 'old' and 'new' SA. The two periods are characterized by different national security policies. Various illustrations showing the difference in national security policy application will be used. For example, prior to 1994, the RSA maintained an aggressive military posture towards its neighbouring countries. This was demonstrated by the South African Defence Force (SADF) raid of Matola in Lesotho 1981, (Bottoman, 2010, p. 60) and further military attacks in Angola and South West Africa in 1975, (Gleijeses, 2002, pp. 229-300) to mention two.

More atrocities are listed in the book *The Honour to Serve* by Ngculu in which he recollects the experiences of an Umkhonto soldier (Ngculu, 2009, pp. 129-131 & pp. 143-147). That there existed a different national security policy pre-1994, compared to the post-1994 situation in SA is further supported by the writings of Nortje in which he describes gruesome battles and wars fought by the SADF prior to 1994 in pursuit of national security under the apartheid regime. The researcher adds his own practical experience of the pre-1994 and post-1994 written policies, as he lived during this era and was actively involved in fighting the discriminatory laws and atrocities of the apartheid regime, as well as having to take part in the preparation for the post-liberation period that saw the CODESA phase.

Post 1994 brought an end to apartheid through a negotiated settlement. This historic moment also saw the national security policy shift from a state only consideration to a pluralistic national security policy. This was illustrated in 1996 by the presiding government at that time as follows:

> 11. *The process of transformation will be guided by the following principles of defence in a democracy. These principles derive from the Constitution and government policy:*
>
> *11.1 National security shall be sought primarily through efforts to meet political, economic, social and cultural rights and needs of South Africa's people, and through efforts to promote and maintain regional security.* (*Defence in a Democracy: White Paper on National Defence*, 1996, p. 6)

> 2. To elucidate this view further, the *White Paper on National Defence for the Republic of South Africa*, states that:

> *After two and a half decades of isolation, South Africa has been welcomed back into the international community and has joined a host of important regional and international bodies. The country's foreign relations have been transformed from an adversarial mode to bilateral and multi-lateral cooperation.*

> *5. This fundamental shift has been accompanied by a dramatic change in the strategic environment at domestic and regional levels. While the potential for instability and conflict remains, the salient fact is that the government is no longer*

unrepresentative and at war with its own people and neighbouring states in Southern Africa.'

8. Among others, its aim and scope include that: *'Defence policy should be in harmony with all other aspects of government policy, particularly foreign policy and national security policy. It can be described as that subset of government policy which is concerned with countering military threats; with the orientation, preparation, maintenance and employment of armed forces; and with the procurement of weaponry and military equipment.* (*Defence in a Democracy: White Paper on National Defence for the Republic of South Africa*, 1996)

The above quotations form the basis for the new military posture and military doctrine to inform the new defence and security structures of the new SA, hence the need for transformation of government state apparatus to suit the new environment and lay the basis for the defence review completed in 2012.

To elaborate on the above subject, the researcher has employed the Global Positioning System (GPS). From the researcher's point of view, its use requires a strategic policy as part of the national security policy because of potential threats to GPS services which would possibly have a negative effect on the RSA's security, defence, political, economic and social arrangements. This is the main reason that inspired the researcher to conduct this study. This need is aligned to the US's National Executive Committee for Space-Based Positioning, Navigation and Timing that constantly undertakes a study on mitigation of threats to the GPS. This view is also expressed by Bartlett (2008).

The researcher recognises the need to enquire whether the RSA has mechanisms in place to deal with threats to the GPS. If so, what are they, and how effective are they? The absence of these mechanisms is of serious concern. For example, it is fairly common that when you draw money at an ATM at irregular intervals, it could take an hour or more for an electronic beep to inform you that a transaction occurred from your account. While driving, the direction-pointer of the GPS sometimes loses signal. What causes these delays?

The Constitution and relevant legislation has given a mandate to the state, particularly the security cluster, to ensure that all security threats are addressed, be they economic, political or social, on behalf of its citizens (i.e. human security) and the state at large.

When clicking on the GPS website, one is welcomed by this wonderful message:

> *The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. The system provides critical capabilities to military, civil and commercial users around the world. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver*.
> (http://en.wikipedia.org/wiki/Global Positioning System, 2013/03/26).

From the researcher's point of view there are five points to underline in the above message.

1. As a consumer or receiver of GPS services, how will you know whether your current location is covered by at least four unobstructed satellites?
2. As it is clearly stated that the system is maintained by the United States government, suppose one cancels one's subscription, what happens to one's connectivity to it?
3. Again as it is said to be free, how does the US benefit from this Samaritan action as we are not ignorant of the costly research and development process that forced the Russian GLONASS system to be partially abandoned in the late 1990s.
4. As it originates from the US military and is still maintained by the US government, what happens when a country is no longer on good terms with the US?
5. What happens to the information already in the possession of the US?

While these are hard questions to be answered in a report like this, it is necessary for GPS users, besides the Americans, to have a clear understanding before subscribing or continuing to enjoy a 'free ride' as presented by the US. Developing states should inform themselves of these matters when thinking and planning around their national security interests. Another factor that should be of concern is the environmental impact these satellites have from their point of being launched to when they are in space, and during their time in space. What is the

level of pollution versus the cost-benefit.. Do developing countries accrue any benefits compared to first world countries. These are some of the questions that require clarity from those who make bold statements that something is for free.

One other critical factor that should inform the RSA political situation regarding its national security is the notion of a Developmental State.

> *A developmental state tackles the root causes of poverty and inequality. A South African developmental state will intervene to support and guide development so that benefits accrue across society (especially to the poor), and build consensus so that long-term national interests trumps short-term, sectional concerns.* (NDP, 2010, p. 53)

To the researcher, notwithstanding the various views or conception held by the term, the concept befits South Africa because of its characteristics that include historical divisions that are racially based, poverty levels, unequal development also based on race, the infant mortality rate, literacy rate, unemployment, Gini coefficient, and policies of its government and political leadership.

Since the 2009 National Elections, the ruling party (ANC), has prioritised five areas namely, education, health, job creation, combating crime and rural development, implying that these should be factored into the basic thrusts of government business.(ANC 2010 Election Manifesto and ANC 2011 January Statement). These are condensed into a government programme named the National Developmental Plan (NDP). The NDP is managed by the National Developmental Planning Commission (NDPC) in the presidency. According to the NDPC, all departmental plans of the government of the Republic of South Africa must be anchored around the NDP, including the national security policy and the national security strategy of SA (ANC 53rd National Conference Resolutions, 2012, pp.22-23).

Therefore, because national security is shaped by local (i.e. domestic), regional and international factors, societal threats posed by the GPS should be equally viewed from these three perspectives of national security policy. Where policy adjustment is required, thorough assessment based on the short and long-term vision should be conducted and, if necessary,

adjusted or changed accordingly because problems facing GPS and related systems will have a negative impact at all three levels that have a bearing on national security at both policy or strategic level and the tactical level of different countries. These perspectives will be discussed later on as regional and international perspectives.

Furthermore, Task 8 of the *SA Defence Review* calls on the Department of Defence (DoD) to ensure the implementation and strengthening of information security. To this end, the following quotation refers:

> *State requirement 90. The risk of South Africa's communications and electronic data being subject to a cyber-attack remains a reality. The protection of Information Bill refers to state information which requires protection against unlawful alteration, destruction, or loss of valuable information.* The quotation goes further to state that *'It is of critical importance that the concept of Information Operations be established on national level to coordinate State activities in the Info Sphere (Figure 60). Information Operations can thus be applied as the coordinating body to ensure that the security cluster and civil society will collaboratively define national information security goals to protect information as a strategic resource.* (South African Defence Review, 2012, p. 211)

Drawing from the understanding of the above quotation, two important words should be underlined, namely; 'the state' and 'civil society'. Through these two concepts, it should be clear that a new paradigm of a development-friendly conceptualisation of national security must be crafted. This further strengthens the need for education about patriotism and sound citizenry, calling for public servants to serve and protect the information of their country diligently. This also applies to civil society. People should realize that as information is power, it must be managed responsibly. Either wittingly or unwittingly, the security of the state may be compromised with the result that national security is compromised, as defined in the new paradigm shift. It is within this context that the issue of risks associated with GPS and related systems must be viewed. What if the sorely needed services of the GPS are suddenly no longer available? All stakeholders of the national security policy should be vigilant to these questions.

To conclude on the cyber-security aspect, the RSA endeavours not to let its people down by crafting and implementing drastic measures. COMSEC Pty Ltd was established in 2002 with the primary responsibility of ensuring that important and sensitive information / communications of the state are secured. Its work should be complimented by the security cluster departments, namely, the SAPS, defence, the State Security Agency, the Department of Science and Technology and the Department of Communications. Each department has designated areas to specialise in. These are explained in the *South African Defence Review* (2012, p. 213).

Lastly, a quote from the policy framework is imperative, as it further demonstrates the extent to which SA's security agencies commit to their legislative mandatory responsibilities:

> *the National Cyber-Security Policy Framework seeks to ensure that Government, business and civil society are able to enjoy the full benefits of a safe and secure cyberspace through working together to understand and address the risks, reduce the benefits to criminals and seize opportunities in cyberspace to enhance South Africa's overall security and safety including its economic well-being.* (Draft National Cyber-Security Policy Framework for South Africa, 2011, p. 15.)

The above statement is profound in the sense that it identifies national security role players and calls them to action to attain a common goal i.e. safety and economic growth while stresses that criminals should be fought by denying them access to vital national security information. To realise the above factors, social infrastructure, communication infrastructure, IT infrastructure and many more should be optimally functional, reliable and secured. Hence, it becomes worrying when there are risks ascribed to a technological apparatus like the GPS.

2.8 AFRICAN CONTEXT

The GPS and GIS can also be utilised regionally in order to minimise costs to be borne by a single country; sharing costs with neighbouring countries is the perspective within which the matter is raised. The European Union (EU), U.S.A, China and India currently do this. A similar process can be implemented in Africa whereby regional bodies such as the SADC and ECOWAS could include the issue of GPS challenges. This, however would rely heavily on trust and cooperation among the member states.

The African situation differs from that of the EU. The possibilities for cooperation are not easy to figure out because at times outside 'forces' such as former colonisers also determine who the enemy is and at what time. For example, the Central African Republic (CAR) military *coup d'état* that left fifteen (15) RSA soldiers dead. France, as a former coloniser, had its interests in the conflict-ridden CAR.

The security systems work better and are more cost effective when they are connected from a country to neighbouring countries then to regional and continental level. However, how is this applied among countries such as the CAR and its neighbours who distrust one other? This situation is unlike that of the Russians who work in collaboration with China and India on the GLONASS, and the EU member states that work together to strengthen the alternative navigation satellite system, the Galileo. A solution to the threat to GPS requires cooperation among neighbouring countries to bring down the cost of research.

Natural endowments get confused with competing interests of other powers. Therefore, the collaborative initiatives are uncertain as to how long will they last or on what criteria they should be based. Military science teaches that one's best friend today may be one's worst enemy tomorrow and vice versa, but it does not matter what kind of situation the country finds itself in, it must ensure that its national security interests are safely guarded. As part of its national security safety, its weaponry, including technological warfare and information-warfare, must tie up with its strategic defence posture / capabilities, which takes one back to the purpose of GPS, GIS, and cyber-space which have pivotal roles to play in the execution of tasks. (*Annual Report*, 2010/11, p. 22).

Neighbouring countries under the Southern African Development Community (SADC) and the Economic Community of West African States (ECOWAS) could collaborate. This is further illustrated by Barber (2005, pp. 1088-1090).

An interesting point to note from the literature is the realisation that as development (i.e. economic, social and political) occurs, new technological advances come to the fore. These successes also unwittingly attract potential threats to the developmental aspects of a country. For instance, when Germany moved from its traditional industrial economy to information technological advancement, new threats surfaced. Information-warfare, cyber-warfare, cyber-

crime and the like started becoming a headache for Germany. This matter is receiving attention by the EU.

A similar situation happened to the USA. As founder of both the e-Loran and the GPS technologies, the country suffered an historic technological attack on the World Trade Centre and the Pentagon on September 11, 2001. The 1941 attack on Pearl Harbour that led to America entering the Second World War, and the 1945 nuclear attack on Hiroshima and Nagasaki are all examples that even technologically advanced countries can suffer because of the use and misuse of technology (Raymond, 2003, p.71). Surely, such incidents should make policymakers and implementers think harder when postulating about future developmental plans pertaining to a national security policy. Issues such as these should inform the national security interests of any country or region.

It is a fact that the integration of systems to produce lethal outcomes are out there in the market. It is up to each country to ensure that its national security is in place and intact. This can be done individually or in collaboration with others. The trend has been to group geographically, e.g. USA working with Canada, South America, Mexico and Brazil. The dilemma, however, is what to do with countries like Cuba with her different ideological outlook from the US? The same can be said about Israel versus Palestine; Russia witnessed perestroika and the glasnost in the late eighties, which affected their GLONASS. Their GLONASS system deteriorated due to lack of adequate funding. The Russian experience should teach that the issue of equipment dealing with security can be better utilised in joint cooperation with neighbouring countries to minimise both the research and development costs and the application or operational costs.
In the discussion of different satellite systems above, costs estimates were given to indicate what financial costs to keep in mind when considering a solution to the threats posed to the GPS. Cooperation and collaboration by countries could lower these costs to an affordable level, especially for the developing states in an effort to improve their situation. This could add a building block to aspired goals leading to the development of the African continent.

A brief discussion follows on the African Union's plan to enhance support for an alternative backup system.

2.8.1 Programme of the African Union (AU)

The AU's programme to build civil infrastructure, geared towards 2030, is encapsulated as follows:

> *A united and integrated Africa; an Africa imbued with the ideals of justice and peace; an inter-dependent and robust Africa determined to map for itself an ambitious strategy; an Africa underpinned by political, economic, social and cultural integration which would restore to Pan-Africanism its full meaning; an Africa able to make the best of its human and material resources, and keen to ensure the progress and prosperity of its citizens by taking advantage of the opportunities offered by a globalized world; an Africa capable of promoting its values in a world rich in its disparities.*
> (http://www.nepad.org/economicandcorporategovernance)

The Commission of the African Union (CAU) set itself the above goal to pursue the AU's vision to:

> *build an integrated Africa, a prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force international arena.*

Among the various priorities contained in these programmes, two remain directly related to GPS namely, Programme Six that deals with a peaceful Africa in a peaceful world.

This programme deals with ten-year border management activities, including the conciliation and arbitration of border issues. This requires a common coordinate reference frame understood by both countries sharing a given border. The Priority Programme 17 'Linking Africa', involves two or more countries in the construction of linkage railway lines like the Cape-to-Cairo and inter-state bridges. For these to be realised, the use of a common coordinating frame of reference is required for the countries involved to communicate effectively. This then led to the setting up of the African Geodetic Reference Frame, which is discussed below as another priority.

2.8.2 African Geodetic Reference Frame project

The African Geodetic Reference Frame (AFREF) was created to unify the geodetic reference frames for more than 50 African countries. AFREF will be used in conjunction with the International Terrestrial Reference Frame (ITRF) and they will both use the GPS. The AUC clarifies this point as follows:

> *The generally accepted international standard reference frame in use today is the International Terrestrial Reference Frame (ITRF) and, once complete, AFREF will be fully consistent and homogeneous with the ITRF which will be the fundamental basis for the national and regional three-dimensional reference networks. When fully implemented, its backbone will consist of a network of continuous, permanent Global Positioning System (GPS) stations such that a user anywhere in Africa would have free access to the data collected at these stations and would be at most 1000km from such stations. Full implementation of AFREF will include a unified height datum for Africa.* (http://geodesy.net/encompass/ncbuilt.ntm)

The weaknesses of the GPS, alluded to in the first chapter, put enormous responsibilities on the AFREF. Therefore, the threats facing GPS should also be a cause for concern to the AFREF. The AUC is to make mission and vision statements and objectives set out by the African heads of state in the New Partnership for Africa's Development (NEPAD) realisable. (http://www.nepad.org/economicandcorporategovernance)

2.9 SUMMARY

To conclude the literature review, it is worth pointing out that the GPS is a critical tool in the environment of defence, security, agriculture, communication, science and technology, mining and sports. Its importance has been drawn from the works of various authors on the GPS and other navigation satellite systems. GPS works in conjunction with GIS. The RSA's defence and security development also hinges on both GPS and GIS. These also have bearing on socio-economic development of the RSA, SADC, AU and other regional as well as continental bodies. Literature consulted revealed the challenges faced by the GPS as well as the risks associated with various navigation satellite systems. It was also affirmed that alternative systems are being investigated by different countries to deal with the weaknesses of the GPS. Countries adopt various strategic approaches to varying conditions.

Therefore, the researcher moves to next aspects of research method used to source information dealing with the study undertaken.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 INTRODUCTION

The research methodology provides a framework indicating the direction the research is going to follow in a cohesive and sequential manner regarding the methods applied. Each method is underpinned by a particular school of thought. There are also various schools of thoughts.

3.2 MIXED METHODS RESEARCH

In this chapter, the methodology used to answer the research question successfully is discussed, including the use of specific methods and data collection techniques. The measuring instruments as well as their reliability and validity are also addressed. The population and the sample used are defined and explained.

The approach taken by this study to address the research question is the Mixed Methods Research, particularly the Convergent Parallel Mixed Methods Design.

Mixed Methods Research is a mixture of both the qualitative and quantitative research methods. It is also referred to as a convergence approach. According to (Creswell, 2014), a Mixed Method Research can be described as having the following characteristics:

- *It involves the collection of both qualitative (open-ended) and quantitative (closed-ended) data in response research questions or hypotheses.*
- *It includes the analysis of both forms of data.*
- *The procedure for both qualitative and quantitative data collection and analysis need to be conducted rigorously (e.g., adequate sampling, sources of information, data analysis steps).*
- *The two forms of data are integrated in the design analysis through merging the data, connecting the data, or embedding the data.*
- *These procedures are incorporated into a distinct mixed methods design that also includes the timing of the data collection (concurrent or sequential) as well as the emphasis (equal or unequal) for each database.*
- *These procedures can also be informed by a philosophical worldview or a theory (see Chapter 3).* (Creswell, 2014, p.217)

Creswell further notes that there are various terms used for this approach which include the '*integrating, synthesis, quantitative and qualitative methods, multimethod, and mixed methodology'.* However, recent writings tend to use the term 'mixed methods (Bryman, 2006; Tashakkori & Teddie, 2010).

These methods date back to the 1980-1990s and draw from the strengths of both quantitative and qualitative research data.

- There are three types of mixed methods designs, namely, the Convergent Parallel Mixed Method Design, Explanatory Sequential Mixed Method Design, and Exploratory Sequential Mixed Methods Design. All these are described using the following framework.

    - 1. *Description of the design*
    - *2. Data collection*
    - *3. Data analysis*
    - *4. Interpretation*
    - *5. Validity* (Cresswell,2014 pp.219-226)

A questionnaire was used to determine what knowledge the research participants have of satellite systems. The questions 1 to 7 were quantitative and questions 8 to 17 were qualitative. The sequencing was to build from one set of information to the next. If a respondent was not familiar with questions 1 to 7 of the questionnaire, it went without saying that he/she may not be empowered to answer the rest of the questions (i.e. questions 8-17) on the prepared questionnaire.

1) Qualitative research approach

A qualitative approach is one in which the inquirer often makes knowledge claims based primarily on constructivist perspectives (i.e. the multiple meanings of individual experiences, meanings socially and historically constructed, with an intent of developing a theory or pattern); on advocacy/participatory perspectives (i.e. political, issue-oriented, collaborative or change oriented); or on both.

Qualitative researchers study things in their natural settings, attempting to make sense of or interpret phenomena in terms of their meanings.

Qualitative research seeks out the 'why', not the 'how' of its topic through the analysis of unstructured information e.g. interview transcripts, open ended survey responses, emails, notes, feedback forms, photos and videos. It does not just rely on statistics or numbers, which is the domain of quantitative researchers.

Qualitative research is used to gain insight into people's attitudes, behaviours, value systems, concerns, motivations, aspirations, culture or lifestyles. It is used to inform business decisions, policy formation, communication and research. Focus groups, in-depth interviews, content analysis, ethnography, evaluation and semiotics are among the many formal approaches that are used, but qualitative research also involves the analysis of any unstructured material, including customer feedback forms, reports or media clips.

The researcher employs the qualitative method of inquiry based on the following value justification:

- *Research that elicits tacit knowledge and subjective understandings and interpretations,*
- *Research that delves in depth into complexities and processes,*
- *Research on little known phenomena and innovative systems,*
- *Research that seeks to explore where and why policy and local knowledge and practice are at odds,*
- *Research on real, as opposed to stated, organisational goals,*
- *Research exploring novel, ignored, or often marginalised populations,*
- *Research for which relevant variables have yet to be identified.*

(Marshall & Rossman, 2011, p. 91)

To briefly explain the relevancy of the above-mentioned values, the researcher will highlight the following:

While many people are aware of GPS, they are ignorant of its weaknesses. The same could be said about military equipment, communication equipment, agricultural implements, transportation and others, that largely use GPS or GIS – linked services. The combination of these technologies is a complex matter, especially for those who do not work directly with the GPS or have not studied these technological subjects. Hence the view that some may have a tacit knowledge about technology, its complexities, its influence or implications to the company policy and the country's national security policy. The research seeks to explore these realities in an attempt to inform the public and stakeholders.

To contextualise the above-cited research values, the researcher is further influenced by the fact that today's societies make use of technology that is reliant on GPS and largely computerised, despite the fact that there are threats to its operations. The motivation for this research inquiry stems from the question whether the country is ready to minimise the aforementioned threats. Therefore, the qualitative research method is preferred in this study and the case study on the GPS. The researcher appreciates and concurs with Marshall and Rossman regarding the values to be realised through choosing the qualitative method cited above.

2) Critical Social Science Theory

> *The primary purpose of Critical Social Science is to conduct studies to critique and transform social relations by revealing the underlying sources of social control, power relations, and inequality.* (Neuman, 2011, pp. 108-109).

To contextualise the above quotation within the research study, it is implied that GPS is the only navigation satellite system founded and used by the American government, yet when studying the literature review it becomes clear that there are other navigation satellite systems, e.g. GLANASS, Galileo, and Compass. This underpins that society, especially developing countries, should not rely on GPS without attempting to either find a backup to it or constructing their own alternative navigation satellite systems because GPS has its own weaknesses. Relying solely on GPS runs the risk of becoming forever dependent on the system despite its weaknesses. It is this social conduct that the researcher intends to critique and correct among societies, especially the newly liberated ones such as South Africa, Mozambique and Namibia. Unless the affected society changes, the USA will remain dominant and countries without alternatives will remain subjected to the US GPS system, despite its shortcomings. The GPS, in its current

form, presents a threat to the national security of SA, especially when viewing/reading the current national security in the context of the new paradigm of national security definition as explained in chapter one.

The explanation forms the basis within which the Critical Social Science (CSS) method is cited as an element that emanates from the Marxist School of thought. The Marxist theory and analysis provides us with an analytic capability called dialectics. *'Marxist theory explains that all changes result from opposing social forces, which come into conflict because of material needs*. (Oxford Advanced Learner's Dictionary, 2010, p. 402)

According to Neuman (2011, p. 110), the founders of this school of thought (Marx & Engels, 1947:39) stated the following:

> *The ideas of the ruling class are in every epoch the ruling ideas … The class which has the means of material production at its disposal, has control at the same time over the means of mental production, so that … ideas of those who lack the means the of mental production are subject to it.*

The Marxist Theory of Analysis pertaining to the GPS is contextualised as follows: The GPS, as the technology of a first world country i.e. America, is currently prevailing over the world through its ideas of the GPS. Developed countries utilise the system and at the same time are in the process of establishing their own technological systems to make up for the weaknesses of the GPS. Developing countries also make use of the GPS, which is recorded as having weaknesses, yet not much is known of what backup technology they have to mitigate the risks of GPS. The researcher used the CSS method of approach to pour light on the situation.

The GPS is an excellent information communication technology tool that has proved its use in the fields for agriculture, mining, transport, communication, and many more. However, this very useful communication tool has weakness or challenges, some of which are natural and some are man-made such as jammers, selection availability, and degradation.

3) Case-study research

According to Yin (1993):

> *The label 'case studies' covers a wide variety of research designs. However different they may be, they have one property in common: they study a social phenomenon by focusing on one case, or at the most, a handful of cases. That is why the label 'small scale research' is also used. Furthermore, in case studies the phenomenon is studied intensively, which is why the label 'intensive research' (in depth) is sometimes used*. (Yin, 1993, p.61)

Based on the above definition by Yin, this study concentrated on people employed in the defence and security related environment as they work either with the GPS or with technologies related to it. This is in line with the problem statement as well as the purpose statement outlined in chapter one.

Neuman (2011, p. 42) states that:

> *case-study research examines many features of a few cases. The cases can be individuals, groups, organisations, movements, events, or geographic units. The data on the case are detailed, varied, and extensive*. … *case study research is an in-depth examination of an extensive amount of information about the very few units or cases for one period or across multiple periods of time*. (Neuman, 2011, p. 42)

The GPS is being studied in this research. It is selected among the Global Navigation Satellite Systems (GNSS), namely; the Galileo Navigation System, the Compass Navigation System, the Indian Regional Navigational Satellite System and GLONASS, established or constructed by different countries at varying times.

According to Neuman (2011, p. 42), the case study method has the following strengths:

1. *Conceptual Validity: Case studies help to 'flush out' and identify concepts/variables that are of greatest interest and move toward their core or essential meaning in abstract theory.* (In the case of this study, the GNSS is the generic term for all the satellite systems being used, with the focus on one of its categories, namely the GPS. The fact that there are other competing systems to GPS such as GLONASS, COMPASS and the Galileo navigation satellite system, broadens the scope and conceptualisation of other possible inventions.)
2. *Heuristic Impact*: *Case studies are highly heuristic (i.e., providing further learning, discovery, or problem solving). They help with constructing new theories, developing or extending concepts and exploring the boundaries among related concepts.* (The mere fact that GPS and GIS can be tasked jointly to produce a point of a particular destination is commendable, but this very important service can be misused which is also an important aspect to keep in mind. Hence, the need to find out what could be a solution to the challenging problems facing GPS.)
3. *Causal mechanisms identification.* (Case studies have the ability to make visible the details of social processes and mechanisms by which one factor affects others. The combination of GPS, GIS and other technological systems that can produce a car hijack, theft, hi-tech crime and cyber-crime, are examples that require a resolve as a way forward in order to enjoy services of GPS and other similar technologies.)
4. *Ability to capture complexity and trace processes: Case studies effectively depict highly complex, multiple-factor events/situations and trace processes over time and space.* (This aspect can, for example, be related to the GPS's being time-bound to the WGS84.The complexities are demonstrated by the inter-linkage and operability of the GPS with other technologies, ranging from the GIS to the jammers, selective availability and the like.) (NGA website.)
5. *Calibration*. *Case studies enable researchers to adjust measures of abstract concepts to dependable, lived experiences and concrete standards.* (As we learn that other countries, like EU, Russia and China are devising plans to mitigate threats similar to those posing to GPS, SA too ought to be ready for any possible challenges that may arise at any point in time.)

6. *Holistic elaboration. Case studies can elaborate on an entire situation or process holistically and permit the incorporation of multiple perspectives or viewpoints.'*

Having read about initiatives that other countries are involved in with regard to GNSS, and observed illustration of the inter-operability of the GPS and GIS, it behoves students, scholars, researchers, practitioners and policy makers in the defence and security environment to assist in finding a resolution to the problem. It therefore, make sense for further study to take place in this field of technology to rescue SA from some of the possible life threatening situations that may exist as a result of the weaknesses of the GPS. Depending on the magnitude of the problem and the direction from which it comes, appropriate responses could be devised using the very same technologies. Case study research was very useful in introducing such valuable concepts in this research study for the national security of a country.

There are different types of case studies, namely, descriptive, explanatory and exploratory. In this case study, both descriptive and explanatory research studies were applied. However, for the purpose of this research, these will only be acknowledged.

GPS, as a technology, belongs to the Modernist school of thought. The researcher cites the Modernist approach because it believes in technology and science, a necessary thinking that has been useful to the problem statement and purpose statement of research undertaken in addressing challenges facing GPS. This school of thought is also cited because it rejects the notion of neutrality in life, thus pointing out that even authors and researchers have a particular underlying philosophy, a view that is also largely shared by the researcher.

The GPS is a modern instrument. It uses modern mechanical instruments with geo-information and science. These are seen through application of GIS, GPS triangulation, WAGS84 to mention a few. The GPS presents an interesting learning experience whereby one aspect of an instrument belonging to one category of school of thought has a bearing on another i.e. GPS as modernist versus Marxist ideas. This school of thought relates to the problems affecting the GPS, as the Marxist school of thought calls upon the need to change peoples' lives by resolving their problems, including those related to GPS in this regard. Hence the interesting scenario of the two schools of thoughts. This motivated the researcher to make use of Case Study Research to review what systems other countries are using to mitigate threats to GPS.

According to Kalof, *et al* (2008, p. 126), a survey method, particularly an in-depth interview method, is constituted mostly of open-ended questions used to obtain descriptive information from the subject or field of study. This is a one-on-one interview whereby in-depth open-ended questions are asked. The disadvantage of this method is that it is time consuming and expensive, as questions have to be prepared and constructed for them to elicit information through answers from the interviewees. However, once this is done, it may be faster to execute. The face-to-face interview method allows the interviewer to probe, clarify and ask follow-up questions. This case study focussed on participants working in the defence and security environment.

What follows next is the research design in which the route conduct research is explained.

3.3 RESEARCH DESIGN

According to Fox and Bayat (2007, p. 51), a research design is the actual plan through which the researcher will get information from the participants or subjects. Therefore, the researcher conducted research following the plan as part of the research design. It had a timeframe like a Gant -chart, indicating what is to be done by who and when.

3.4 DATA COLLECTION

Data collection can be conducted using either primary data or secondary data or both. The researcher used the data collection method through semi-structured interviews. Some questionnaires were emailed to participants and appointments to conduct face-to-face interviews were made with other participants. The researcher targeted individuals in various institutions that use GPS or technologies related to it.

The interviews were conducted as follows:

The researcher identified companies that use GPS and similar technologies and ser up appointments telephonically. He introduced himself to managers and explained the purpose of the research, the questionnaire and its usefulness to the company and the country at large in view of national security. To put the manager at ease, the researcher produced his security clearance certificate and explained that this was a voluntary exercise and that strict confidentiality regarding all information would be observed.

The researcher arrived on time for the interview. He met the manager and discussed issues face-to-face. The researcher clarified the purpose of the study and explained the questionnaire. The manager then completed the questionnaire on his own on his computer. The researcher had already sent the questionnaire electronically.

When the participant was done, he escorted the researcher to the workshop where he was introduced to the technician. Again, the researcher introduced himself, outlined the purpose of the study and the confidentiality issues and explained that this was a voluntary exercise. He produced his security clearance identity, went through the questionnaire with the participant then left the participant to complete the questionnaire manually. The respondent completed the questionnaire, asking clarity where he needed to, until it was done. The researcher thanked him and proceeded to the next appointment where the exercise was repeated.

Although the explanation of the above scenario may appear simple and straight forward, an immense amount of work went into it. For example, appointments were made via the telephone, the aim of the interviews were explained and rapport was built in the process. On the day of the interview, direct contact was made with the respondents through one-on-one interviews based on the questionnaire. The researcher then followed the managers to the workshop to meet their operational personnel and the researcher was allowed to interview one staff member. There was an element of observation as the interviewer interfaced with personnel in a working environment i.e. in their workshop with technologies related to GPS. This kind of interview was applied to five interviewees. By presenting the same questionnaire to the respondents in the manner stated above, the researcher was able to achieve triangulation. According to Neuman (2011, p. 164), triangulation is '*the idea that looking at something from multiple points of view improves accuracy*'.

3.4.1 Personal data

The respondents provided their personal information as follows:

- Name and surname
- Job title
- Company name
- Telephone numbers
- Email address

- Highest educational qualifications
- Race
- Gender

This information helped to establish what knowledge the respondents had pertaining to GPS and related systems. For example, as most of them were engineers, the questions revealed in which fields of engineering they worked e.g. engineers in IT, electrical, technical specialist, integration technician, NTD industrial, and B Eng (Mech). The same order was followed when asking questions ranging from personal information to enquiries about their field of study pertaining to GPS and other technologies. This kind of question sequencing is useful for data analysis (Creswell, 1014, p. 224).

The questionnaire further probed the respondents' position in the company. The information included the following:

- Position held in the company or organisation
- Number of staff reporting to you
- Number of managers reporting to you
- How long have you been appointed in this position
- Total years of working experience in the company/organisation
- Estimated number of employees.

Based on the above information, the researcher could confirm that the selected sample indeed worked with technical and engineering related systems. The respondents were fairly aware of the workings of the GPS or systems related to it. This created trust and confidence in the information they provided.

3.4.2 Organisational data

The researcher required the participants to indicate the categories / organisations they worked for, for example, defence, public service administration, or private company. The reason for obtaining this specific information was to have an understanding of the participant's place of work in order to establish whether she/he was in a position to provide meaningful information

or answers to the questions posed pertaining to the research. The organisational data was also useful in assessing the participants' knowledge of GPS or related systems.

Depending on the respondent's responses, the researcher could determine their usage of the GPS or similar systems in their environment. This also assisted the researcher to assess their knowledge regarding challenges, problems and risks associated with the PNT systems in operations. If respondents were unable to answer questions or were unfamiliar with the questions in this category, they were unable to answer the questions in the next category. This was proved by the response from a participant who was unable to answer questions in this category. The respondent had no knowledgeable of the GPS or similar systems and was equally unable to provide answers to the qualitative questions as the researcher delved deeper into the research subject (see respondent number 2). Conversely, the participants who were able to provide information on both personal and organisational data were also able to provide responses to qualitative research questions. (See respondents' responses from 1-9.)

Based on the above information, a deduction was made that both the personal data and the organisational data served as a necessary and useful preface to the actual qualitative research questions addressed next.

The reasons for selecting these subjects varied, although the purpose was similar, i.e. to collect data. For example, SANDF, through the army and navy, works within the environment that uses technology similar to the GPS and some equipment that is GPS-linked. This was explained at the international event held in SA, the 3rd Indian Ocean Naval Symposium from 10-13 April 2012 in Cape Town. Thus, relevant technocrats or operatives who took part in the research process were quite helpful.

People from intelligence, the police and defence were selected because the matter under discussion falls within the ambit of their departments and they have a pivotal role to play in this regard.
Other important and relevant subjects included the Department of Science and Technology and defence-related industries such as the Advanced Technology Engineering (ATE) and the CSIR.

In administering the research, the researcher guarded against possible biases that could have swayed his reliability and validity.

3.5. PRIMARY DATA AND SECONDARY DATA

3.5.1. Primary data or sources

Primary data refers to articles such as letters, diaries, newspapers, movies, clothing and equipment, including persons who may be still alive, capable of narrating the given story or information. (Mouton, 2001, pp. 69-70). In this case, interview questionnaires were used to gather information in which the respondents wrote their views. Thus, their written views were largely obtained and used as sources of information.

3.5.2 Secondary data or sources

In addition to the qualitative interviews, the researcher used secondary data, such as qualitative documents like public documents including newspapers and official reports or private documents such as personal journals and e-mails, the Constitution of RSA, acts and policy documents, (Creswell, 2009, p. 181; Mouton, 2001, p.71). The researcher also used newspapers such as the *City Press*, the *ArcUserMagazine* for Esri Software Users, and the internet for different internet websites and books.

3.6 QUALITATIVE SAMPLING DATA USED.

Certain procedures are to be followed by the interviewer or researcher when conducting an interview. There are also various ways to conduct an interview, for instance by telephone, web surveys and face-to-face interviews. Each method has both advantages and disadvantages that were taken into account in executing the study. Telephonic interviews were used in preparation for the face-to-face interviews.

3.7 VALIDITY AND RELIABILITY:

3.7.1. Validity

> *Validity means trustfulness. In qualitative studies, we are more interested in achieving authenticity that realizing a single version of 'Truth'.* (Neuman 2011, p. 214)

Information was collected by sending questionnaires via email to a focus group in the defence and security industries and through interviews using a structured research questionnaire. These

were completed by the respondents by hand or typed and are available for inspection and verification, as are their contact details. Validity was realised through person-to-person interviews and observation that assisted with triangulation. The triangulation in this regard was through the quantitative results combined with the qualitative summary of the report outcome, as they both confirmed the existence of threats to GPS–linked services. These results are shown with graphic illustrations (see Table 1, history gram 1 and the pie chart (Creswell, 2014, pp. 222-223)

3.7.2. Reliability

> *Reliability means dependability or consistency. We use a wide variety to techniques (e.g., Interviews, participation, photographs, document studies) to record observations consistently in qualitative studies. (*Neuman, 2011, p. 214)

Reliability measurement is the kind of measurement tool that can be relied on under the same circumstances. For example, a bathroom scale, upon weighing oneself repeatedly after bathing, gives the same reading, assuming that one has not overindulged, can be said to be a reliable measuring tool. Thus, the information collected using the methods already cited under validity above can be relied upon, as it was confirmed during visits to the premises of the participants through pre-arranged appointments.

3.7.3. Interpretation

Having used the Mixed Method Research study, the interpretation of the results took cognizance of both the quantitative and qualitative results. The next chapter will illustrate how both results concurred.

3.7.4. External and internal validity

According to Creswell (2014), external validity threats arise '*when experimenters draw incorrect inferences from the sample data of other persons, other settings, and past or future situations'.* As a researcher, one has to guard against this possibility. Another threat is the internal validity threat that refers to the experimental

> *inabilities of the researcher to follow proper procedures, treatments, or experiences of the participants that threaten the researcher's ability to draw correct inferences from the data about the population in an experiment* (Creswell, 2014, pp. 174-177)

Regarding the validity and reliability of the information given by the respondents, it is given that most, if not all, the participants in the research are professional people. Information was supplied voluntarily, so their information can largely be trusted. A respondent would have no benefit in inflating his/her qualification because he/she is not applying for a job or gaining anything, except perhaps the results of the research study report.

The information from questions 1-7 can be accepted as correct as it is general in nature. As a result, one can say that there is validity and reliability in their information answers. All responses to question 1 & 2 indicated familiarity with the question content. Most importantly, it must be noted that questions 1-7 are of a quantitative nature as a prelude to the qualitative research method of approach to the research. The approach was mixed i.e. a combination of a quantitative and qualitative research method. It can also be termed a side-by-side approach or a side-by-side comparison whereby the researcher makes a comparison of statistical data within the discussion. As not many statistical figures were involved, the research cannot rightly qualify as quantitative research, hence the maintenance of the mixed method research method of study (Creswell, 2014, pp. 222-223)

As can be verified from the completed questionnaires, each respondent answered the rest of the questions differently while explaining his / her viewpoint. Thus, from the researcher's point of view, the information presented through the research report is valid and reliable.

3.8 SUMMARY

In conducting the research study, the researcher employed a Marxist school of thought in general and Critical social science theory in particular. A mixed method approach where a quantitative and qualitative is used and sequencing of these has been followed. Personal, career and organizational data was sourced sequentially as this is useful for data analysis. The aspects of data validity and reliability were also given necessary attention. Hence data collected is sufficient and prudent for analysis as it is to follow next.

CHAPTER FOUR: RESEARCH FINDINGS

4.1 INTRODUCTION

This chapter presents the research outcome based on the questions asked by the researcher to the interviewees or respondents. After drawing up the questionnaires and circulating them to the respondents, their inputs were received and summarised into the formats in which they are presented. Out of the 17 questionnaires issued, 11 were returned. The questionnaires comprised qualitative questions, premised by questions about the professional or work experience of each participant. Thus, the sample was drawn largely from individuals working in defence and security related-departments and industries who work with the GPS and related systems. In order to anchor the questions, some personal information was asked at the beginning of the questionnaire. These were introductory questions, as the thrust of the research was based on qualitative research. However, their information was critical, as the data analysis shows. This kind of question sequencing revealed the participant's knowledge of the subject (i.e. the GPS and its weaknesses).

4.2 QUANTITATIVE QUESTIONS

These questions range from 1 to 7 (see table 1 below).

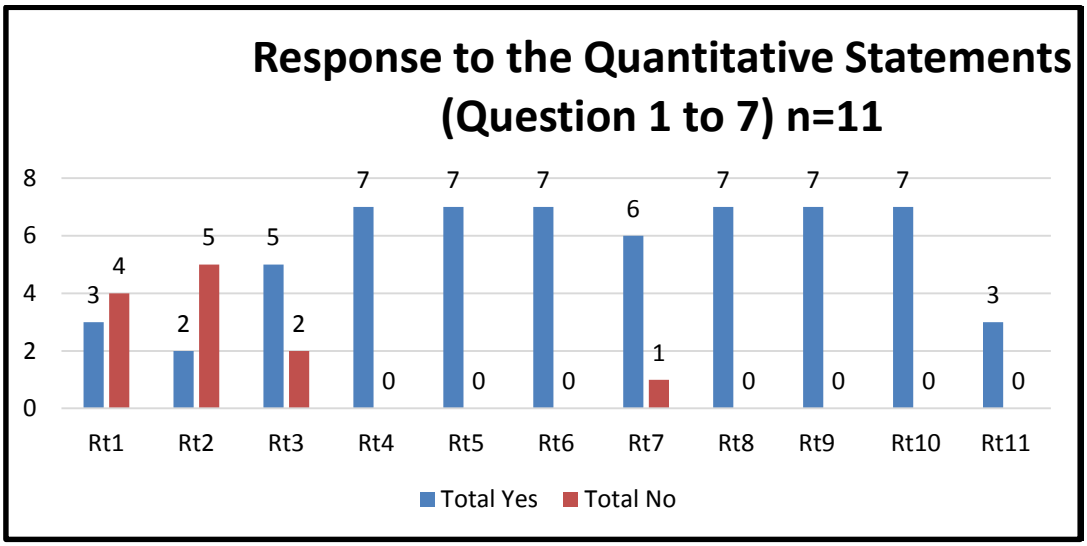
Coding**:** The data collected is coded using two digits. The digit one (1) reflects a 'yes' and digit two (2) reflects a 'no' response. A non-response was assigned a digit nil (0). The respondents' real names were replaced by numbers 1 to 11 to protect their identity. Information required about navigation systems and concepts is meant to lay a foundation for the research and is presented as follows:

Table 1.

Serial	Rt1	Rt2	Rt3	Rt4	Rt5	Rt6	Rt7	Rt8	Rt9	Rt10	Rt11
1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1	1
3	1	2	2	1	1	1	2	1	1	1	1
4	2	2	2	1	1	1	1	1	1	1	0
5	2	2	1	1	1	1	1	1	1	1	0
6	2	2	1	1	1	1	1	1	1	1	0
7	2	2	1	1	1	1	1	1	1	1	0
Total Yes	3	2	5	7	7	7	6	7	7	7	3
Total No	4	5	2	0	0	0	1	0	0	0	0

The information from Table 1 is presented in a histogram below

Histogram 1.



By placing the above data into a histogram, it is evident that respondent number 1 agreed with three statements out of the seven. . However, the majority of the respondents responded affirmatively to the seven questions. There were also statements to which the respondents did not provide any response, these are reflected as a zero (nil). The results suggest that out of the 11 participants, there is a level of appreciation regarding information management technology used in position navigation systems.

TABLE 2: Depicting the familiarity of GPS/GIS (i.e., Qs I & Qs 2) and other concepts (Qs 3-7)

Q	Rt1	Rt2	Rt3	Rt4	Rt5	Rt6	Rt7	Rt8	Rt9	Rt10	Rt11
1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
3	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y
4	N	N	N	Y	Y	Y	Y	Y	Y	Y	0
5	N	N	Y	Y	Y	Y	Y	Y	Y	Y	0
6	N	N	Y	Y	Y	Y	Y	Y	Y	Y	0

7	N	N	Y	Y	Y	Y	Y	Y	Y	Y	0
TL	Y3/ N4	Y2/ N5	Y5/ N2	Y7	Y7	Y7	Y6/ N1	Y7	Y7	Y7	Y3

Notes: 1. Q: Questions; Rt: Respondent(s); Y: Yes; N: NO and TL: Total and 0: No Response.

2. All 11 respondents are familiar with both GPS and GIS therefore among this population, GPS and GIS is popular / familiar.
3. Most of the respondents are familiar with Q3-7 (i.e. 8 out of 11)
4. This information is essential for the purpose of a cost-benefit analysis to make an informed decision regarding services rendered by these systems.
5. The information is important in asking the next questions about the participants knowledge of the threats or weaknesses facing GPS.

Qualitative questions

Question 8

Respondents were asked to name the systems they use in their companies or organisations. Table 2 below represents the participants' responses.

TABLE 2: Depicting Systems used in various departments / companies in SA.

Rt1	Rt2	Rt3	Rt4	Rt5	Rt6	Rt7	Rt8	Rt9	Rt10	Rt11
GPS	GPS	GPS	GPS	CSI	GPS	GPS	None	GPS	GPS PNT CDM	0
	Kiwit system					GIS	none			
	Vulture system									

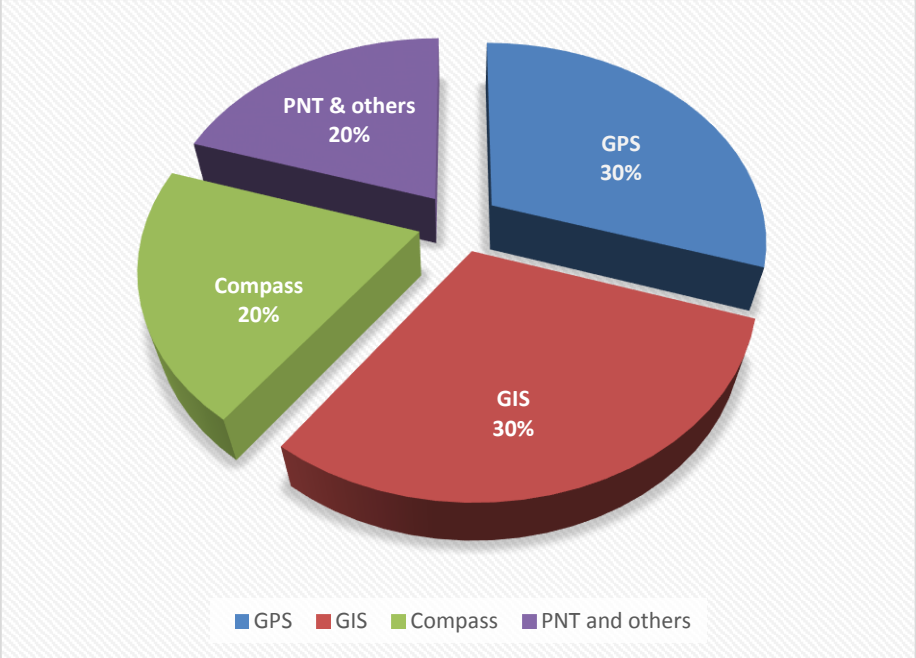
Notes:

- Systems used in SA are as important as those used in other countries in terms of the assessing their services, capabilities and problems likely to be encountered in operational fields.
- Both GPS and GIS are mostly used in the defence-related industries, followed by Compass and other PNT systems and CDM.

- Thus, as GPS and GIS can be deployed / used combined, it is essential for its users to look out for any possible threats that may affect their capabilities.

Graphic presentation depicting the above-mentioned scenario:

Pie chart 1.



Notes:

1. Both the GPS and GIS are mostly used, followed by Compass and other PNTs.
2. Any potential threat to either the GPS or GIS is ominous for their services to continue. (See also table 2 above.)
3. There is still room for further development in this area. New system entrants and cooperation could be done.

Any interference or disturbance of these systems will cause problems for SA. Therefore, South African leaders, policymakers, policy analysts, technical engineers and managers in the defence and security environment need to advise their principals accordingly so that SA can close the gap or seize the opportunity to invest in this field, especially when compared with the response to Question 9 below.

Question 9

TABLE 3: Depicting value to each system

Rt1	Rt2	Rt3	Rt4	Rt5	Rt6	Rt7	Rt8	Rt9	Rt10	Rt11
GPS	GPS		GPS	GPS	GPS	GPS		GPS	GPS	GPS
GIS	GIS		GIS	GIS	GIS		GIS	GIS		GIS
			PNT		PNT		PNT	PNT	PNT	PNT
							Galileo			
	Compass Magnetic		Compass							
			WAAS							
			CDM	CDM	CDM		CDM	CDM	CDM	CDM
Electro-optical			Electro-optical	Electro-optical	Electro-Optical		Electro-optical	Electro-optical		Electro-optical
			Flex-System							
			Multi-Mode		Multi-Mode			Multi-Mode		
UAVs	UAVs		UAVs	UAVs	UAVs			UAVs		
			Space-satellite-based	Space-satellite-based	Space-satellite-Based			Space-satellite-based		

Notes: From table 3 above, we can deduce that the GPS and GIS are the most valued systems compared to the rest, followed by the CDM Electro Optical, CDM, Electro-Optical, UAVs and Flex Multi-mode. Therefore, a threat to GPS services will indeed cause serious damage to areas where it is mostly used, i.e. in transport, communication, defence, security, agriculture and mining.

Question 10: are you familiar with the weaknesses of the GPS?

This question was asked to establish the respondents' familiarity with the weaknesses of the GPS.

Rt1	Rt2	Rt3	Rt4	Rt5	Rt6	Rt7	Rt8	Rt9	Rt10	Rt11
Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y

Notes: 10 out of 11 respondents answered yes, this means almost all these participants know / are aware of the problems facing GPS as they named them under the sub-question to question 10.

Rt1	Rt2	Rt3	Rt4	Rt5	Rt6	Rt7	Rt8	Rt9	Rt10	Rt11
Jamming U.S.A control	**0**	**0**	Deception control of powerful powers	Signal loss	Denial deception Jamming	Manipu-lation Super power	Position updated through satellite	Denial deception and jamming	Deception on satellite commu-nication & political factor	

Notes: 8 out of 11 respondents attribute the weaknesses of GPS to jamming, deception, lost signal, political control, disruption and intrusion. Thus, above 75% of the personnel working in various areas are aware of the challenges to GPS.

However, 2 out of 11 respondents (Rds, 2&3) are unaware of the GPS weaknesses. This, means that the majority of the participants are aware of the weaknesses; they even named some of the weaknesses, as mentioned earlier. This finding corroborates the assertion that the GPS has indeed got weaknesses.

The above finding also leads to the purpose statement, which was to establish whether SA has a risk mitigation factor to deal with weaknesses facing the GPS system. This finding further provides justification for the requirement of a backup system to counteract the weaknesses of the GPS as mitigation factors to the risks.

The findings led to the research questions enquiring about the SA situation regarding these risks versus the mitigation means. These were expressed in questions 12 to 17, the qualitative research method questions are explained below.

Most of the respondents attribute financial costs to be the main reason for lack of alternative backup to GPS

Question 14

What system would be the ideal for South Africa?

Notes: In summary, one respondent out of nine did not respond (respondent no 2); one said she/he saw no use (respondent no 8); others saw no problem with GPS usage (respondents 3&4); one noted the possible US threat, but felt that the GPS is still the best (respondent no 7); the rest, (respondents 6, 5 & 1) propose the use of GPS in combination with other systems such as GNSS or Galileo.

Question 15

GPS: Are there any benefits to be accrued by SA for ensuring that it has a reliable GPS?

Notes: Most of the respondents indicated 'Yes' it is feasible for SA to have an alternative system to GPS by considering other systems and by collaborating with other institutions through R&D, etc.

Question 12: Why does South Africa not have a backup to the GPS system?

Rsd1	Rsd2	Rsd3	Rsd4	Rsd5	Rsd6	Rsd7	Rsd8	Rsd9	Rsd10	Rsd11
Don't know	No re-sponse	Too ex-pensive	RED required	Costly	Education problem	Costly	No need	Lack of education	Costly	Unaware of potential threats

Summary notes

1:2 = Don't know

2:4 = Educational problem about GPS functionality and knowledge about potential threats.

3:2 = Research and development required.

4:3 = Costly excuse

Question 13: **Is it feasible for SA to have its own standalone PNT?**

Rsd1	Rsd2	Rsd3	Rsd4	Rsd5	Rsd6	Rsd7	Rsd8	Rsd9	Rsd10	Rsd11
Don't know	No answer	Yes, but costly	Yes, but costly	No, costly	Yes, but costly	No	No	Yes, but costly	No	Yes, but costly

Summary Notes

1. Do not know=3
2. Yes but costly=5
3. No=3

Question 14: What system would be ideal for SA?

Rsd1	Rsd2	Rsd3	Rsd4	Rsd5	Rsd6	Rsd7	Rsd8	Rsd9	Rsd10	Rsd11
No specific choice	No answer	GPS	GPS	Hybrid of GNSS/ GPS etc.	GNSS	GPS	No opinion	Localised aerostat based argumentation systems	Combination of different service providers	e-Loran

Summary Notes

3= GPS

2= No opinion

3= Hybrid systems

1= e-Loran

1= No answer

1= GNSS

Question 15: GPS: Are there any benefits to be accrued by SA for ensuring that it has a reliable GPS?

Rsd1	Rsd2	Rsd3	Rsd4	Rsd5	Rsd6	Rsd7	Rsd 8	Rsd9	Rsd10	Rsd11
Self-control in time of crisis	No answer	Yes, accurate self-timing	Yes, in line with protocols	Yes, enhance accuracy and reliability	Yes, military viewpoint	Yes, if reliability can be assured	Yes	Yes, from military viewpoint	yes	Yes

Notes 1. The majority of participants said there will be benefits and only two were not sure. It means SA should indeed pursue research and development and utilise more than one system, as to its strategic nature that has to be affirmed.

Question 16: How can SA ameliorate itself in respect of challenges facing GPS?

Rsd1	Rsd2	Rsd3	Rsd4	Rsd5	Rsd6	Rsd7	Rsd8	Rsd9	Rsd10	Rsd11
Utilize multiple systems GLONASS, Galileo, GPS, etc.	NO answer	No idea	Research development to find alternative GPS	Research and development very important	Form alliance with other countries	Afford-ability	Re-search cheaper, low cost system	Use GNSS not only GPS	Use differed services providers	Installing PNT backup in case GPS failure

Notes: Six respondents (1, 4, 5, 6, 8 and 9) are of the view that SA should conduct R&D, form alliances with other institutions on the similar / related systems. One did not respond (respondent no 2) and another one said 'No response' (respondent no 3). One respondent saw this as a mission that was not achievable (respondent no 7). Therefore, the majority in the sample are pointing to a need for further research about the various systems and possible new inventions.

Most say SA must do more research and others say SA must use multiple systems.

Question 17: Are your company's intervention strategies sufficient to mitigate threats posed to the GPS?

Rsd1	Rsd2	Rsd3	Rsd4	Rsd5	Rsd6	Rsd7	Rsd8	Rsd9	Rsd10	Rsd11
Hybrid techniques employed	No view	No view	Various systems	-	None	No	N/A	no	yes	No

Summary notes

6= No views

2= Use hybrid systems

1= Not applicable

1=Yes, have means

After the presentation of these research responses to questions (i.e. Q1-17), the following summary deductions are made below.

Qualitative data responses

In an attempt to ensure that the respondents had a full understanding of what the statements in the questionnaire suggest, a follow-up session was arranged between the researcher and the respondent. The questions asked were aimed at identifying the systems used by the respondents within their own environments, their familiarity with them as well as the flaws they have identified (See Appendix A, Questions 8 to 17). The researcher recorded the responses which were subjected to a qualitative thematic data analysis process. The following themes surfaced:

(a) Challenges facing the GPS
(b) Costs and affordability of the alternative systems as a backup to GPS.
(c) The role of research and development as a means to mitigate risk factors for GPS and related systems.
(d) Economic and social benefits.

4.3 DEDUCTIONS

4.3.1 Quantitative responses:

Due to the sensitivity and nature of the study, the names of the eleven participants were excluded as per the consent to participate form signed prior to the data collection. As a result, the data is coded using fictitious names to protect the participants. At the same time, to concretise the findings, the researcher uses a mixed method (i.e. both quantitative and qualitative data gathering methods) especially with regard to Questions 1 to 7.

The data indicates that 55% of the participants are fully conversant with the ICT used around them.

4.3.2 **Qualitative responses**:

- It was revealed that respondents who are knowledgeable about the PNT Systems (including GPS & GIS), are able to provide some ideas on solutions to challenges facing GPS, whereas those who do not know much about the PNTs, also do not have any solutions to the challenges facing GPS.
- Even some of the respondents who are somewhat knowledgeable about the GPS or GNSS generally, do not know how to deal with the challenges facing the GPS.
- Only participants who demonstrated their knowledge about the GNSS / PNT system were able to provide possible solutions to the challenges facing the GPS.
- A category of respondents who are knowledgeable about the GNSS / PNTs and who are aware of the challenges facing GPS, preferred not to provide any alternative view towards the possible solutions to the problems facing the GPS. There seems to be a reason for holding back their views with regard to possible solutions. This assertion is arrived at, because due to their knowledge, qualifications, skills and their work experience, they should have the capacity to provide at least some possible solutions facing the GPS.
- In the main, it was established that SA uses several systems. While this is good, the risks are highly possible and it would also be difficult to trace which system is failing the country. The GPS is one of the systems popularly used despite the threats mentioned.
- Most respondents recommended that further research should be conducted as a solution to faulty GPS.
- On the issue of an alternative to the GPS, the respondents recommended collaboration with other countries to find a solution. This could save South Africa some research resources, but that SA should have research skills for the project.

According to Neuman (2011), interviewer behavioural bias must be avoided; these include but are not limited to those cited below:

- *Errors by the respondent.*
- *Unintentional errors or interviewer sloppiness.*
- *Intentional subversion by the interviewer.*
- *Influence due to interviewer's expectation.*
- *Failure of an interviewer to probe or to probe properly.*

- *Influence on the answers due to the interviewer's appearance, tone, reaction to answers, or comments made outside the interview schedule.*
  (Neuman, 2011, p. 347.)

The researcher tried to avoid falling victim of any of the above. However, interviewer bias is not easy to detect, therefore, it is left to the readers of this report to judge, on the clear understanding that it was unintentional.

Issues from the respondents' responses are identified and grouped, according to their relativity, into themes which are discussed next.

4.4. THEMES

Themes emanating from the research findings are named below:

(a) Challenges facing the GPS
(b) Costs and affordability of the alternative systems as a backup to GPS
(c) The role of research and development as a means to mitigate risk factors for GPS and related systems
(d) Economic and social benefits.

The research findings are discussed in the next chapter on data analysis to be carried out following the themes that emerge from the report, as already alluded to above.

4.5 SUMMARY

In this chapter, the researcher conducts analysis on the distinct data from quantitative questions and the qualitative questions paying attention to particular findings. It is from the findings that the researcher draws deductions. These deductions are then categorised into themes that forms the basis of data analysis.

CHAPTER FIVE: DATA ANALYSIS

5.1. INTRODUCTION

This chapter is largely informed by the findings of the research questionnaires. It should be noted that a qualitative research study method was used in this study. The historical background of SA informs the context within which the research is conducted and the changed environment calls for a change in the way the national security has been conceptualised. A survey using written questionnaires was done on a focus group i.e. a smaller number from 1 to 11, for only 11 out of 17 distributed questionnaires were returned (70%).

A content analysis and intensified interview technique was applied in the qualitative method. A content analysis technique was applied to the written information about the GPS and various alternative systems, and a comparison with different countries at different times, was made to establish their different alternative PNTs and or GNSS systems.

These established facts were analysed and synthesised into themes that emerged from the respondents' inputs in the previous chapter. Only some of the emergent themes will be discussed, especially those having a direct bearing on the purpose of the research.

5.2. DISCUSSION OF THEMES

Data analysis involves preparing the data for analysis, conducting different analyses, moving deeper into understanding the data, representing the data and making an interpretation of the larger meaning of the data (Creswell, 2003, p. 190).

Questions 1 to 7 are background questions to gather information about the knowledge, ability and suitability of the respondents in the research focus group. This helped to establish that they are all professional people at varying post-tertiary levels, ranging from post-matric diplomas to masters degrees, from ordinary technicians to middle and senior managers.

The following themes emanated from answers to questions 10, 12, 13, 14, 15, 16 and 17:

A. Challenges facing the GPS
B. Costs and affordability of the alternative systems as a backup to GPS.
C. The role of research and development as a means to mitigate risk factors for GPS and related systems.
D. Possible economic and social benefits.

A number of these themes are discussed below:

A. Challenges facing the GPS

A deductive approach analysis and an illustration is used to introduce the challenges facing the use of the GPS.

For example, whilst driving your vehicle, the GPS signal is lost and you lose directions to where you were going. This usually happens when you are surrounded by high buildings, bushy areas or mountains leaving you stranded and insecure, depending on how familiar you are with the area. This happens as a result of limitations of the GPS.

According to Barlett (2008), the GPS has some weaknesses such as loss of signal which causes the above situation. This view is shared by the National Executive Committee for Space-Based Positioning Navigation and Timing System (*Ingenia*: Issue 34 March, 2008).

As a solution to these problems, some respondents answered, 'Investigate access to new-generation alternative systems to GPS being developed internationally' i.e. that a formal alliance within IBSA / BRICS member state countries be investigated for approved access to alternative GPS / PNT system as an option.

Some respondents suggested that the development of an autonomous PNT system within the prioritised objectives of the National Space Agency and security cluster priorities should be considered. As South Africa is part of BRICS and IBSA, economic opportunities presented by these bilateral and multilateral agreements and Memoranda of Understanding (MOUs) should be explored to share knowledge about technologies in this environment.

Other weaknesses identified by the respondents include:

- Loss of signal in some African terrains (i.e. dense bushes, mountains and indoors)
- Can be spoofed to give false readings.
- USA controls it and can deny signals to the rest of the world if need be.
- Denial, deception jamming and outdoor only.

The above research findings confirm that there are threats to GPS such as jamming, loss of signal especially in high buildings, underground, and bushy areas, a fact that is supported by what was found earlier through research studies conducted by reputable bodies in this field of GPS. (Barlett, in *Ingenia:* Issue 34 March 2008 and the National Executive Committee for Space-Based Positioning, Navigation and Timing)

This signifies the importance with which threats to the GPS service must be viewed by the security cluster and security sector; it also confirms the researcher's problem statement, purpose statement, and research questions. The risks include those emanating from cyber-security such as cyber-crime, cyber-warfare and hi-tech crime.

B. Costs and affordability of alternative systems

It is a common understanding among scholars, the private sector and government sector that to undertake research require resources, therefore the inputs made in this research should under no circumstances be read with the impression that whatever is suggested will be without challenges.

A cost-benefit analysis should be done weighing the risks of continuing to use the GPS without attending to the alluded potential threats with creating a budget for resources required to ameliorate SA from the situation. The crux of the matter is that only one of the two can be done with dire consequences for each. On the one hand, research brings costs, while on the other hand one can live with the *status quo*.

As largely explained in chapter two, there are those such as the security cluster, who have a Constitutional mandate to be in line with the new paradigm of national security.

Note should be taken of various cost implications given under the various systems as initiatives have already been taken or are in the process of being implemented by various countries. Further desk research on why these systems are so costly was explained in chapter two.

Cooperation between and among countries is of paramount importance. Without overstating the point made previously, the US is reported to be working with China and India on the same subject. EU countries are also working together to deal with their situation regarding their Galileo navigation satellite system. The above stated comparative information is informed by the empirical analysis done during the literature review, where costs implications were revealed country by country under every navigation satellite system mentioned.

South Africa, therefore, can consider undertaking the same mission by tabling the matter with SADC member states, before proceeding to ECOWAS and others. This is important considering the physical conditions of the continent of Africa. Economic and political conditions, including the influence of the former colonisers, will also have a bearing on the proposed initiative. Some respondents proposed that SA should take the matter up as suggested above to meet costs and counteract the alluded threats.

The new paradigm of the concept of national security places a responsibility on the state as well as society at large (i.e. state and human security) to implement, manage and take pre-cautionary measures to enhance national security.

C. Role of research and development as a means to mitigate risk factors for GPS and related systems.

Most respondents recommended that further research be conducted as a solution to the faulty GPS. Regarding alternatives to the GPS, the respondents recommended collaboration with other countries to find a solution. While this could save South Africa some research resources, it raises another issue that needs further research.

The GPS is used in various areas including transport, security networks, agriculture, mining, maritime, communications and military warfare. These are crucial areas for South Africa's economic development and the GPS will further improve the South African productivity level in

a reliable and sustainable manner. However, with the weaknesses that have been alluded to, all GPS users should pay attention to these challenges by creating a backup mechanism.

Each country needs to find an alternative system to the GPS. The US as the founder of the GPS system, spends relentless efforts on research and development to monitor the performance of the GPS and to work on its weaknesses so that it can continue to earn them a good return.

From the respondents' input, there is no doubt about the challenges facing GPS. Even among those who are familiar with challenges, there is an issue as to how to resolve these problems. The respondents demonstrated that while they have knowledge of the GPS systems functionality and importance, they answered that they do not know how to resolve the problem i.e. although these problems are within their area of work as engineers or technicians, they do not have the expertise so solve these challenges. It was noted that the respondents who have no knowledge of either the GPS or GIS are unaware of the challenges facing the GPS.

Some of the respondents could be giving the above responses (don't know) truly because they really do not know, but some could be withholding their knowledge and expertise for various reasons. Nonetheless, these responses take us back to the original reasons for conducting a research study - a need for a backup system to mitigate risks facing the continued reliance in the use of the GPS.

Certain respondents thought that perhaps SA should continue to use the multiple systems as a mitigating factor to challenges facing GPS. Their explanation implies that some of the challenges could be reduced/ avoided.

Other respondents indicated that SA should provide more resources for research and development to find a solution. They mentioned that SA could do so in collaboration with other countries, which is an approach similar to that of China's collaboration with Russia and India, and the US's collaboration with China and Russia in an effort to tackle weaknesses facing the GPS.

The respondents who are familiar with the GPS rank both the GIS and GPS as very valuable, while some respondents who are unfamiliar with either the GPS or GIS, value the systems and some do not. When combining all the respondents, it is clear that the majority of the respondents value the GPS.

An information gap was revealed, as the respondents who work with GPS related systems showed that they are ignorant of the challenges facing GPS. This finding compounds the nature of the problem we have in South Africa. As this is not the aim of this study, further research may be required.

The risks associated with technology related applications of GPS include hi-crime, cyber-crime, and cyber-warfare.

D. Possible economic and social benefits

The researcher looks at a way of addressing the prevalent GPS threats as a means to partly deal with SA's socio-economic problems, as these threats involve national security.

As mentioned previously, the GPS system was established for defence purposes in the US in 1978 and has since been expanded into civilian use in transportation, telecommunications, agriculture, mining etc. (Pham, 2011, p. 3). The GPS is also used by insurance companies to track vehicles and monitor vehicle mileage compliance with contractual agreements between the insurance companies and the vehicle owner or user (Bartlett (2008, p. 37). These factors could persuade the South African authorities and policy implementers to consider the spin-offs to investing in solving threats posed to GPS services. The private sector also stands to benefit in this venture that will grow the economy.

It is necessary at this stage to be reminded of the geographical location of SA and the areas of its security responsibilities:

- Total air border: 7 660km
- Total land border: 4 471km
- Total maritime border: 3 924km
- Total EEZ area: 1 553 000 km^2

- Total land surface: 1 219 090 km^2
- Total maritime area: 4 340 000km^2

(*SA Defence Review*, 2012, p. 133)

To protect and secure all these areas various technologies are used, including those linked to GPS. To illustrate the magnitude of the threat, when adding up all the borders and areas to be secured, 14 221 180km are open to technological threats. This exceeds the size of Europe, a developed country that is already involved in the Galileo positioning satellite navigation system.

As some of these areas are manned by technological systems that are GPS linked, it would have a devastating effect on the economy and social aspects on all South Africans if the GPS is threatened. Conversely, as the GPS is also used in communication, transport and agriculture for example, SA will accrue gains from the reduction of threats to the GPS.

Goolam Ballim, the Standard Bank's chief economist, and Simon Freemantle, the head of Standard Bank's African Political Economy Unit, agree that with SA being part of BRICS, it opens economic opportunities for the country. *'More broadly, the Brics affiliation gives South Africa a scaffold to recalibrate its growth potential.'* (*The Star*, business report, March 25, 2013) Therefore, the researcher is of the opinion that South Africa should also use the opportunity to foster research and development in order to close the gap regarding threats to the GPS. The above suggestion comes because China, Russia and India are involved in such initiatives to mitigate threats to the GPS.

5.3. CONCLUSION ON DATA ANALYSIS

There are clear summary findings that confirm some weaknesses already alluded to in the literature review. Based on the literature review and case studies conducted, it is now factually correct to confirm that GPS has weaknesses that include jammers, loss of signal in high vegetation areas such as forests, or near high buildings. Possible threats stemming from political control by the originating country of GPS have also been confirmed. Denial and deception are ascribed to the originating country of the GPS. Further research on alternative systems is recommended on how SA can ameliorate itself from the challenges affecting GPS. Clearly, SA should start putting together its own navigation satellite system; partnering with other countries being among many options to be considered. The issue of costs was raised as

a further challenge that needs to be addressed. In conclusion, SA and other developing states have possibilities than can be considered. Some of the options are explained in the recommendations.

The various themes and how they flow into one other has been discussed. In the next chapter, the researcher proceeds to summarise the research findings and make recommendations.

5.4 SUMMARY

Having conducted data analysis above, four themes have been identified, namely:
Challenges facing the GPS; costs estimates of alternative systems; the role the research and development could play in minimising risk factors and possible economic and social benefits for reduction of risks facing GPS. It is indeed worthwhile to pay a considerable attention to given data analysis. Hence, the recommendations as outlined in the following chapter.

CHAPTER SIX: SUMMARY AND RECOMMENDATIONS

6.1. INTRODUCTION

Having concluded an analytic assessment of the research findings, the researcher now recommends what must be done taking into account the literature reviewed and the research method underpinned by a particular school of thought which led to research findings. Thorough consideration was given on what has been done in terms of research studies by other research bodies and the practical experience of those in organisations or companies involved in the defence / security industry that use or are familiar with the GPS or with systems related to it.

6.2. SUMMARY

There is a need for further research about, amongst others, ownership of the systems and their operability, as this is vital for South African socio-economic development. Even more worrying is that some African air spaces are used by external countries to mount their satellites without the knowledge of African countries, while these countries accrue possible benefits.

Apart from the material benefit due to those countries whose air space is being abused, their national security is being infringed, including their independence and sovereignty. The literature demonstrates that different satellite navigation systems exist and that more are being developed, especially in the developed countries that have collaborative developmental programmes. Perhaps it is time this is an opportunity that is worth consideration by the South Africa and her counterparts. This leaves room for SA to consider initiating a system of its own in pursuance of its Constitutional mandates, including domestic and foreign or international policies within the context of national security policy.

> *Human security needs to be situated in relation to state or national security. A fundamental point of departure is to see to it neither as an alternative to or, nor divorced from, national or state security. From a human security perspective, the security of the state is not end in itself: it is a means of providing security for the people. Thus, human security complements state security in four important respects:*
>
> - *Its concern is the individual and the community rather than the state.*

- *Menaces to people's security include threats and conditions that have not always been classified as threat to state security.*
- *The range of actors is expanded beyond the state alone.*
- *Achieving human security includes not just protecting people, but empowering people to fend for themselves.* (UN Commission on Human Security 2003:4) (du Pisani, 2007, p.18.)

This absence of a backup to GPS presents a threat to both the state and society. The state should address this matter urgently as it leads to other threats such as cyber-crime and hi-tech crime that present threats to life. These are issues that perhaps prior 1994 were not that critical but, like Germany, the US, and Japan, as was explained in the literature review, SA's inauguration of democratic government in 1994 presents challenges that are not exclusive of national security threats.

6.3. RECOMMENDATIONS:

In view of the challenges facing GPS, which also pose a threat to South Africa's national security, it is necessary for the security sector to conduct research to address some of the challenges. It would be prudent to utilize this process to strengthen policy decisions, transform or reform the defence/security sector, and redefine concepts and policies to improve the implementation of the National Security Policy of South Africa.

- The public and authorities in particular, need to inform themselves concerning the challenges in PNT systems, including the GPS. This is a necessary civic duty for any nation to avoid complacency and to encourage innovation.
- Legislative bodies such as parliament, legislatures and councils, should be appraised about these matters and include civil society structures in the security cluster.
- Improvement of the national security policy may develop South Africa's economic, social and political environment. Therefore, the security cluster should implement this recommendation. In addition to policy formulation, skills development should be addressed.
- Although the research focussed on the SA situation, its outcome is highly relevant and useful to any country, especially those beyond SA's borders. Its outcome should inform both private as well as public policy practitioners. Various opportunities are open for consideration. For instance, as was suggested by some respondents, the possibility of

having access to new-generation alternative systems to GPS should be investigated. This is being developed internationally.

- A formal alliance within IBSA / BRICS for approved access to an alternative GPS / PNT system can be investigated.
- The development of an autonomous PNT system must be placed among the prioritised objectives of the National Space Agency and security cluster of SA government. As South Africa is part of BRICS and IBSA, the economic opportunities availed by these bilateral and multilateral agreements and Memoranda of Understandings (MOUs) should be explored. It is imperative for the Security Cluster to take the matter up with their respective counterparts in other countries.
- Cyber-warfare cannot be dismissed as a possible threat, especially through the technological gadgets we carry with us such as cell phones, computers, GIS, GPS, mobile and movable properties. Cyber-security and other security-related systems remain critical for the defence and security environment. This imperative was also emphasised in the *Defence Review* with regard to defence posture in times of difficulty as stated below:

> *Should the need for the deliberate self-defence of South Africa arise, the principle of 'forward defence' will be applied. Should peaceful means and deterrence fail or the level of aggression preclude a peaceful resolution, South Africa will use appropriate and focused force, in partnership or autonomously to:*
>
> *a. Defend itself against aggression*
> *b. Protect its people*
> *c. Protect its sovereignty*
> *d. Protect its territorial integrity*
> *e Protect its national interests and critical infrastructure*.
> (SA Defence Review, 2012, p. 123)

Therefore, security cluster departments must prioritise the matter as it is within their mandatory purview.

- Research and development needs to be improved in terms of scope, funding, capacity and the communicating of results. Ignorance and complacency must be discarded. Laws and policies cannot be static, as these must be identified and improved on to suit prevailing conditions while taking cognisance of developments in the environment. Issues of joint ventures, skills transfer and through public private partnerships that are a purview of DENEL, ARMSCO, and other defence industry companies who must all work together in this environment. The recommendation must be acted upon by the Department of Defence, DENEL, ARMSCO, Department of Science and Technology, Department of Communications, SSA and SAPS.

- Regarding the purpose of the research study, it has been established that whereas it is acknowledged that GPS has weaknesses, and that largely most of the first world counties are engaged in research studies to improve their technological systems, they are also cooperating and collaborating to find a solution to the threats. For example, the regional and continental governance structures. Therefore, SA, SADC, AU, NEPAD, PAP and the like, must act in the spirit of the Common African Defence and Security Policy (CADSP) and Peace and Security Council (PSC) to implement the recommendation.

Specialised skills development

Cognisance should be taken that policy makers (politicians, members of parliament, senior personnel, policy experts and more) are not policy implementers. The implementers comprise people such as engineers and technicians in IT. This categorical distinction is made deliberately to draw a separation between training / education programmes required for each category. Whereas the first category should be well trained in policymaking and oversight, the implementers must be properly trained in implementation skills. Engineering and IT High-Tech skills are required to make a meaningful, practical implementation contributions in the in SA. Policymakers, evaluators and monitors also require the appropriate skills to perform their responsibilities. South Africa needs doers! Therefore, the security cluster should take the lead in the implementation of this recommendation.

Additional areas still need to be researched, such as the actual geographic location of the satellite constellations, the non-interference with state sovereignty of other countries, and the commercial benefits on the space zone. An assessment needs to make as to what extent the

national security of satellite hosting or mounted country is being compromised, especially in developing countries, if indeed it is being compromised. This is in consideration of environmental issues that might also have an impact on their development in the short or long-term, directly or indirectly from the perspective of sustainable development, thus resulting in endless Kyoto protocols. Therefore, SA, SADC and the AU member states should implement this recommendation to further the realisation of a New Economic Partnership for African Development (NEPAD).

Thus, it is prudent to first focus on the issue of the GPS itself. It is good, useful and, if well maintained, its users will draw more benefit from it. However, on the other hand, it is equally problematic because it can be jammed, manipulated by its founders, lose signal in and near high buildings, bushy areas or near mountains to mention a few.

6.4. CONCLUSION

Security, as a concept, is not static. The concept has been debated largely in the defence, security and social arena where human security was part of the discourse.

> *The narrow and simple-minded concept of security exclusively based on the interests of state actors, has gradually given way to conceptualisations and interdependencies amongst the various social actors and structural elements involved in security policies* (Jung, 2009, p. 8).

This notion that should inform national security policy to take cognisance of the role of the GPS and challenges countries are likely to face without a backup.

Tied to the identified challenges, both the Modernist philosophy as well as the Marxist school of thought should constantly remind us that these technological problems affect the people, and it is the people who should embrace technology as well as resolve these problems / challenges.

As indicated in the introduction, everyone from the ordinary person in the street to academics, bureaucrats, leaders, managers, policymakers and policy implementers, are entrusted with the responsibility to ensure that the hard earned democracy that gave birth to the Constitution and legislative mandates still has to be translated into reality.

The researcher concludes by quoting from the inspirational inaugural speech delivered by the first democratically elected President of SA, Nelson Mandela:

> *I have walked that long road to freedom. I have tried not to falter. I have made missteps along the way. But I have discovered the secret that after climbing a great hill, one only finds that there are many more hills to climb. I have taken a moment here to rest, to steal a view of the glorious vista that surrounds me, to look back on the distance I have come. But I can only rest for a moment, for with freedom comes responsibilities, and I dare not linger, for my long walk is not ended.* (Mandela, 2002, p. 751.) (See also businessballs.com).

REFERENCES

Ball, N. & Fayemi, J. K. (ed.) (2004) *Security sector governance: A handbook.* Chapter 1: Introduction. The Case for Security-Sector Transformation, pp. 1-16. Place: Centre for Democracy and Development

Ballim, G. & Freemantle, S. (2013) Opinion: Bricks membership opens opportunities, Johannesburg, *The Star*.

Barber, J. (2005) The new South Africa's foreign policy: principles and practice in *International Affairs* 81, 5 (2005) 1079-1096.

Bartlett, D. (2008) *Ingenia* Issue 34. http://www.pnt.gov

Betz, D.J. & Stevens, T. (2011) *Cyberspace and the state: Towards a strategy for cyber-power.* Abingdon: Routledge.

Bottoman, W.W. (2010) *The making of an MK cadre*, South Africa: LiNc Publishers.

Branigan, S. (2005) *High-tech crimes revealed*, Cape Town: Pearson Education, Inc.

Bryden, A. & Olonisakin, F. (ed.) (2010) *Security sector transformation in Africa*. London: Transaction Publishers.

Chochiouros, I.P. Chochiouros, .S.P. Spiliopoulou, A.S., & Lampadari, E. (2008) Public key Infrastructures as a Means for Increasing Network Security in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber Warfare and Cyber Terrorism*. Hershey: Information Science.

Ciampa, M. (2010) Security awareness: Applying practical security in your world, Brazil, Cengage Learning, www.cengage.com/global.

Clarke, R.A. & Knake, R.K. (2010) *Cyber war: The next threat to national security and what to do about it.* New York: Harper Collins Publishers.

Creswell, J.W. (2009) *Research Design: Qualitative, quantitative and mixed method approaches*. Thousand Oaks: Sage Publications.

Creswell, J.W. & Plano Clark, V.L (2011) *Designing and conducting mixed methods research*. Thousand Oaks. Sage Publications

Creswell, J.W. (2014) *Research Design: Qualitative and quantitative and mixed method approaches*. Thousand Oaks: Sage Publications.

Curren, K. Mclntyre, S. Meenan, H. & Heaney, C. (2008) Electronic Surveillance and Civil Rights in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber Warfare and Cyber Terrorism.* Hershey: Information Science.

du Pisani, A. (2007) Democratic Governance and Security: A Conceptual Exploration, in Cawthra, G, du Pisani, A and Omari, A, Security and Democracy in Southern Africa, Johannesburg, Wits University Press.

Fox, W. & Bayat, M.S. (2007) *A guide to managing social research*. Cape Town: Juta & Co. Ltd.

Franklin, D. (2010) *Cyberpower and national security* Place: National Defence University.

Gleijeses, P. (2002) *Conflicting missions: Havana, Washington and Pretoria*. Johannesburg: GALAGO Books.

Janczewski, L.J. & Colarik, A.M. (2008) *Cyber Warfare and Cyber Terrorism*, Washington: Information Science.

Jones, S. (ed.) (2002) *The decline of the South African economy*. Cheltenham: Edward Elgar.

Jung, D. (2009) Security: Some Critical Observations about Concepts and Policies in Cawthra, G. (ed.) *African security governance emerging issues*, Johannesburg, Wits University Press Available at: http://witspress.wits.ac.za.

Kalof, L. Dan, A. & Dietz, T. (eds.) (2008) *Essentials of social research*. New York: McGraw Hill Open University Press.

Kegley, C.W. (2003) *The new global terrorism: Characteristics, causes, controls.* New York:Prentice Hall.

Kierkegaard, S.M. (2008) EU Tackles Cybercrime, in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber warfare and cyber terrorism*. Hershey: Information Science.

Kilroy, R.J. (2008) The U.S Military Response To Cyber Warfare in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber warfare and cyber terrorism*. Hershey: Information Science.

Knapp, K.J. & Boulton, W.R. (2008) Ten information warfare trends in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber wWarfare and cyber terrorism*. Hershey: Information Science.

Knetzger, M. & Muraski, J. (2008) *Investigating high-tech crime*. New Jersey: Pearson Prentice Hall.

Laqueur, W. (2008) 'Postmodern Terrorism' in Kiegler, The New Global Terrorism: Characteristics, cause, controls, New Jersey, Pearson Education.

Leipnik, M.R. (2008) Use of Geographic Information Systems, in Janczewski, L.J. & A.M. Colarik (eds.) *CyberWarfare and cyber terrorism*. Hershey:Information Science.

Libicki, C.M. (2010) *Conquest in cyberspace: National security and information warfare*. Cape Town: Cambridge University Press.

Mandela, N.R. (2002) *Long walk to freedom: the autobiography of Nelson Mandela*. London. Abacus.

Marshall, C. & Rossman, G.B (2011) *Designing qualitative research*. United State of America, SAGE Publications Inc.

Mokhele, T. & Otto, K. (eds.) (2011) *Leveraging Technology to enhance Situational Awareness: East African Coastal Maritime Awareness Network*. Cape Town: Executive Centre for Sea Watch.

Mouton, J. (2001) *How to succeed in your master's and doctoral studies*, Pretoria: Van Schaik Publications.

Neuman, W.L. (2006). *Social research methods: Qualitative and quantitative approaches*. New York: Pearson Publishers.

Neuman, W.L. (2011). *Social research methods: Qualitative and quantitative approaches*. New York: Pearson Publishers.

Ngculu, J. (2009) *The honour to serve: Recollection of an Umkhonto soldier*, South Africa, David Phillip Publishers

Nortje, P. (2006) *32 Battalion: The inside story of South Africa's elite fighting unit*, South Africa, Zebra Press.

Nugent, J.H. & Raisinghani, M. (2008) Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber warfare and cyber terrorism*. Hershey: Information Science.

Owen, R.S. (2008) Infrastructures of Cyber Warfare in Janczewski, L.J. & Colarik, A.M (eds.) *Cyber warfare and cyber terrorism*. Hershey: Information Science

Pham, N.D. (2011) *The economic benefits of commercial GPS Use in the United States, and the cost of potential disruption*. Available at: http://www.saveourgps.org/voice-your-concern.aspx.

Raymond, G.A. (2003) 'The Evolving Strategies of Political Terrorism' in Kergley, C. The New Global Terrorism: characteristics, causes, controls, New Jersey: Pearson Education

Roane B. Theft by jamming car remotes is on the rise, say insurers, p.6, *Pretoria News*, Friday October 2013 www.pretorianews.newspaperdirect.com

Rowe, N. C. (2008) Ethics of Cyber War Attacks, in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber warfare and cyber terrorism*. Hershey: Information Science.

Ruley, J. (2003) Newsletter of Friday, 11th May 2012 *based on Avionics Report*. South Africa, University Press.

Schoeman, M (2007) 'South Africa' in Cawthra, G, du Pisani, A and Omari, A. Security and Democracy in Southern Africa, Johannesburg, Wits University Press.

Stanaway, R. (2007) GDA94, ITRF and WGS84 what is the difference? Working with Dynamic Datums, Australia, Spatial Sciences Institute.

Stiglitz, J. E. (2006) *Making Globalization Work*. USA, Penguin.Group(USA)

Struwig, F.W. & Stead, G.B. (2001) *Planning, designing and reporting research.* Cape Town: Pearson Education South Africa.

Warkentin, M. Schmidt, M.B. & Bekkering, E. (2008) Steganography in Janczewski, L.J. & A.M. Colarik (eds*.) Cyber warfare and cyber terrorism*. Hershey: Information Science.

Warren. M.J, (2008) Terrorism and the Internet, in Janczewski, L.J. & A.M. Colarik (eds.) *Cyber warfare and cyber terrorism*, Hershey: Infomation Science.

Web site: http://www.eurospanoline.com Retrieved

Pratt, M. (2012) ArcUser: *The Magazine for Esri Software Users* Fall 2012 vol. 15. No. 4. New York, Esri at. Website: (esri.com/arcuser) Retrieved ..

African National Congress 53rd National Conference Resolutions, Mangaung, 16-20 December, 2012.

Building a better world: The Diplomacy of Ubuntu. *White Paper on South Africa's foreign policy,* Final draft – 13 May 2011.

Business Day, 12.13.2004, Johannesburg.

City Press, 24 March, 2013, p.27, Johannesburg.

Defence in a Democracy: White Paper on National Defence for the Republic of South Africa, 1996.

South African Defence Review: White Paper on National Defence for the Republic of South Africa, 2012.

Department of Defence (2011) Annual Report to Congress: Military and Security Developments involving the People's Republic of China, USA, Office of the Secretary of Defence.

Draft National Cyber security Policy Framework for South Africa, 2011.

http://a64214259/GandG/tr8350_htmi

http://en.wikipedia.org/w/indexhttp://www.eurospanon.com

LORAN. (2012, May 13) In Wikipedia, Free Encyclopaedia. *LORAN's Capability to mitigate the impact of a GPS outage on GPS position, navigation and time applications*, March 2004.

National Security through Technology: Technology, Equipment, and Support for UK Defence and Security, 2012, White Paper, London, UK, TSO (Stationery Office).

National Development Plan 2030, National Planning Commission, The Presidency, Republic of South Africa.

The Constitution of South Africa, Act 108 of 1996.

The Interim Constitution of South Africa, Act 200 of 1993

The Oxford Advanced Learner's Dictionary (2010) 8th edition, New York, Oxford University Press.

The South African Police Service Act, 1995, South Africa.

www.businessreport.co.za www.globalcomsatphone.com/hughesnet/satellite, retrieved on 14 September 2013 9:03 pm

ANNEXURES

1. A copy of a letter to potential research participants
2. Copy of research questionnaire

Dear Ms / Mr / Dr _____

My name is Benjamin Ntuli and I am a University of the Witwatersrand student enrolled for a Master Degree in Management in the field of Security. One of my tasks is writing a research report that requires me to consider challenges that face GPS as well as other systems related to it. I would really appreciate your help with this.

The assignment requires me to request ordinary employees, middle management and top management respondents to complete the attached questionnaire. This will take approximately 45 minutes of your time. Your feedback will enable me to compare theory with application and will enhance my understanding of both the practical and theoretical perspectives of the system.

Your participation is voluntary and information will be treated as confidential. In addition, I am in possession of a security clearance and I am aware of the MISS Document requirements. If you are willing to help I would be grateful if you would be so kind as to complete the attached questionnaire and return it to me via this e-mail address (Benjamin.ntuli@dpsa.gov.za). Please note that you may also be contacted by the University to confirm your participation.

Attached, please find a supporting letter from my University.

Thank you

Somangamane Benjamin Ntuli
Student number: 9208912X
Contact details: **Mobile**: 082 496 8349
Email: Benjamin.ntuli@dpsa.gov.za

QUESTIONNAIRE

ABOUT YOURSELF

Personal details (please fill in your details)

Name and surname	
Job title	
Company name	
Telephone number	
E-mail address	
Highest qualification	
Race	
Gender	

Your position within the company / organisation (please fill in your details)

Position held within the company	
Number of staff members reporting directly to you	
Number of managers reporting directly to you	
How long have you been appointed in this position?	
Total years' work experience	
Total years management experience	
Estimated number of employees employed by the company you work for	

ABOUT THE COMPANY / ORGANIZATION YOU WORK FOR

In which industry do you work? Please select only one option.

Agriculture, defence, security, hunting, forestry and fishing	
Mining and quarrying	
Manufacturing	

Electricity, gas and water supply	
Construction	
Wholesale and retail trade	
Transport, storage and communication	
Financial intermediation, insurance, real estate and business services	
Community, security, social and personal services	
National government	
Provincial government	
Education	
Other (please name)	

The following question requires you to think about the Geographic Positioning Systems (GPS), the Geographic Information Systems (GIS) and any other Position Navigation Timing Systems (PNT'S), and other concepts you use in your company/ organization. In answering the question you need to consider the following (simply tick the appropriate boxes):

Questions	Yes	No
1. Are you familiar with the GPS?		
2. Are you familiar with the GIS?		
3. Are you familiar with the PNT's?		
4. Are you familiar with Cybernetics?		
5. Are you familiar with Cyberspace?		
6. Are you familiar with Cyber warfare?		
7. Are you familiar with information warfare?		

QUANTITATIVE

QUESTIONS

Please indicate the value your company or institute attaches to the following systems					
9. If you **use the system**, please indicate the value you attach to it					
	I am not familiar with the system	**I am familiar with the system but we do not use it**	Of no value	Limited value	Highly valuable
GPS					
GIS					
E-Loran					
PNT					
	I am not familiar with the system	**I am familiar with the system but we do not use it**	Of no value	Limited value	Highly valuable
GLONASS					
Galileo					
COMPASS					
WAAS- Wide Area Augmentation System					
CDM – Code Division Multiple Access					
Electro- optical / infrared sensors					
Flex – system for synchronization in a message system					
Multi-mode radar synthetic aperture radar					

	I am not familiar with the system	**I am familiar with the system but we do not use it**	Of no value	Limited value	Highly valuable
GPS – essential for timing and positioning					
Airborne-tethered aerostats, UAVs Aircraft manned-fixing helicopters					
Space-satellite-based sensors – imagery for vessels, oil pollution (deliberate/acci-dental) bathymetric space charts, weather, waves ,currents communications, etc.					
10. Are you familiar with the weaknesses of the GPS system?	Yes	No			
If yes what are the weaknesses?					
11. Other systems: Which of the above systems are you familiar with which has weaknesses you know of and what are they?					

QUALITATIVE QUESTIONS:	
12. Why does South Africa not have a backup to the GPS System?	
13. Is it feasible for SA to have its own independent stand- alone positioning, navigation and timing system (PNT)?	
14. What system would be the ideal for South Africa?	
15. GPS: Are there any benefits to be accrued by SA for ensuring that it has a reliable GPS?	
16. How can South Africa ameliorate itself from challenges facing the GPS?	
17. Are your company's intervention strategies sufficient to mitigate threats posed to the GPS?	

END