Social Media Intelligence (SOCMINT) within the South African context: A theoretical and strategic framework for the national security environment

JI Stegen

orcid.org 0000-0002-8420-999X

Thesis submitted in fulfilment of the requirements for the degree *Doctor of Philosophy in Development and Management* at the North-West University

Promoter: Prof A Duvenhage

Co-promoter: Prof MN Wiggill

Graduation ceremony: May 2019

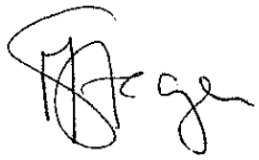
Student number: 22443770

DECLARATION

I, Johanna Isabella Stegen (Student Number 22443770), hereby declare that the thesis entitled:

Social Media Intelligence (SOCMINT) within the South African context: A theoretical and strategic framework for the national security environment submitted in fulfilment of the requirements for the degree, Doctor of Philosophy in Development and Managment, at the North-West University, is my own work and has never been submitted by me to any other university. I also declare that, as far as possible, all the sources used have been acknowledged by means of complete referencing.

I understand that the copies of the thesis submitted for examination will remain the property of North-West University.



Signed……..on this day 16th of November, 2018

DEDICATION AND ACKNOWLEDGEMENT

This thesis is dedicated to my late father, Hermann Stegen, who gave up so much to take care of me and my brother.

I wish to express my sincere gratitude to:

- My Creator for giving me the strength, knowledge, ability, perseverance and opportunity to complete this mammoth task.
- My family and friends for their encouragement, support and understanding over the last five years. It was particularly during the homestretch that your constant cheers helped me across the finishing line.
- My study leader, Professor André Duvenhage, who methodically and with great care and consideration advised and motivated me to produce this thesis.
- My co-study leader, Professor Marlene Wiggill, for your guidance, expertise and understanding.
- Dr Thys van den Berg for being my sounding board and for all the support, assistance and encouragement during this time.
- Christien Terblanche for your assistance with the editing and bibliography.
- Simone Roos for your assistance with the technical aspects of the thesis.
- The librarians for your support and expert advice.
- My employer for giving me the opportunity to develop and make a contribution to this old profession.

ABSTRACT

We are currently living in a complex global environment where change is a given, constantly fuelled by the increasing pace of technological development. These developments affect every aspect of society, including business, education, communication and government. One of the most significant technological developments in recent decades, especially in relation to information communications, is the rise of the internet. This development has brought with it an information revolution that increased the amount of available information, enhanced access to information and reduced the cost of communication. One of the most significant developments associated with the internet is the emergence of social media, which changed traditional communication, augmented social interaction and made state boundaries irrelevant.

The phenomenon of social media plays a key role in the production and dissemination of information and people's access to it. Characteristics such as interactivity, affordability, availability, facelessness and a lack of censorship have increased the use of social media as a tool of communication. These same characteristics also make it attractive to terrorist and other criminal organisations. The implications for national security make social media important for intelligence organisations. This new development motivated this study.

Social media provides the intelligence community with a vast quantity of information (SOCMINT) that could be of importance in safeguarding national security. However, the intelligence community in South Africa is not using this tool to its full potential. The primary aim of this study was to develop a strategic framework for the national security environment in South Africa that includes SOCMINT as a source of information. The secondary aim was to contribute to the theoretical foundation for intelligence studies. This is a young academic field with a limited theoretical foundation and the detailed meta-theoretical discussion in this study adds to the theoretical base of intelligence studies. The proposed framework could enrich the activities of the intelligence community and enhance the intelligence product delivered to the client. This in turn will help ensure the intelligence organisation's relevance in this global environment of information overload.

KEY TERMS: apartheid, communication studies, cyber space, digital age, intelligence, intelligence studies, international studies, internet, national security, new media studies, political science, security studies, SOCMINT, social media, surveillance, technology

OPSOMMING

Ons leef tans in ’n komplekse globale omgewing waar verandering ’n gegewe is wat gedurig aangevuur word deur die vinnige spoed van tegnologiese veranderings. Hierdie verwikkelinge in die tegnologiese omgewing beïnvloed elke aspek van ons samelewing, byvoorbeeld besigheid, opvoedkunde, kommunikasie en die regering. Een van die grootste bydraes uit die inligtingstegnologie-omgewing is die internet. Dit het ’n inligtingsrevolusie meegebring wat toegang tot inligting verhoog het, die koste van kommunikasie verlaag het en die hoeveelheid inligting vermeerder het. Die ontwikkeling van sosiale media het ’n verdere revolusie meegebring. Hierdie nuwe verskynsel het tradisionele kommunikasie verander, sosiale interaksie vermeerder en vergemaklik, en staatsgrense irrelevant gemaak.

Sosiale media speel ’n sleutelrol in die produksie en verspreiding van inligting en mense se toegang daartoe. Eienskappe soos interaktiwiteit, lae koste, toeganklikheid, beskikbaarheid, anonimiteit en gebrek aan sensorskap het die gebruik van sosiale media as ’n kommunikasiemiddel aangevuur. Dit is ook hierdie eienskappe wat die gebruik van sosiale media onder terroriste en kriminele organisasies gewild maak. Hierdie implikasies vir staatsveiligheid maak sosiale media ’n prioriteit vir intelligensie-organisasies, en dit is wat hierdie studie gemotiveer het.

Sosiale media bied aan die intelligensiegemeenskap ’n groot hoeveelheid inligting (sosiale media-intelligensie – SOCMINT) wat belangrik is vir die handhawing van nasionale veiligheid. Hierdie belangrike middel word egter nie tot sy volle potensiaal gebruik binne die Suid-Afrikaanse intelligensie-omgewing nie. Die hoofdoel van die studie was daarom om ’n strategiese raamwerk te ontwikkel wat SOCMINT in die Suid-Afrikaanse intelligensiegemeenskap insluit. Die sekondêre doel was om ’n bydrae te lewer tot die teoretiese basis van intelligensiestudies. Die akademiese veld is jonk en het ’n gebrekkige teoretiese basis, en die gedetailleerde metateoretiese bespreking wat ingesluit is by die studie lewer ’n bydrae tot die teoretiese onderbou van intelligensiestudies. Die voorgestelde raamwerk sal van waarde wees vir die intelligensiegemeenskap met betrekking tot hulle werksaamhede en sal die produk wat aan die kliënt gelewer word, verbeter. Dit sal verder ook verseker dat die intelligensie organisasie relevant bly in die huidige omgewing waar inligting in oorvloed beskikbaar is.

SLEUTELTERME: apartheid, kommunikasiestudies, kuberruimte, digitale era, intelligensie, intelligensiestudies, internasionale studies, internet, nasionale sekuriteit, nuwe media studies, politieke wetenskappe, sekuriteitstudies, SOCMINT, sosiale media, tegnologie

LIST OF ABBREVIATIONS

ANC	African National Congress
ARPA	Advanced Research Project Agency
BOSS	Bureau for State Security
CCSI	Cabinet Committee on Security and Intelligence
CI	Counter-Intelligence
COMINT	Communications Intelligence
COMSEC	Electronic Communication Security
COSMOS	Collaborative Online Social Media Observatory
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DIS	Department of Intelligence and Security (African National Congress)
DMI	Department of Military Intelligence
DONS	Department of National Security
DPCI	Department of Priority Crime Investigations
HUMINT	Human Intelligence
ICT	Information Communication Technology
ID	Intelligence Division
IMINT	Imagery Intelligence
IoT	Internet of Things
IT	Information Technology
MASINT	Measurement and Signature Intelligence
MK	Umkhonto weSizwe
NAT	Department of National Intelligence and Security
NCC	National Communication Centre
NCIS	National Crime Intelligence Service
NI	National Intelligence
NIA	National Intelligence Agency

NICOC	National Intelligence Coordinating Committee
NIE	National Intelligence Estimate
NIIB	National Intelligence Interpretation Branch
NIS	National Intelligence Service
NP	National Party
NSMS	National Security Management System
OIC	Office for Interception Centres
OSINT	Open Source Intelligence
PC	Personal Computer
PCRM	Party of Communists Moldova
RI	Republican Intelligence
RICA	The Regulation of Interception of Communications and Provision of Communications-related Information Act (70 of 2002)
SADF	South African Defence Force
SANDF	South African National Defence Force
SAP	South African Police
SAPS	South African Police Service
SASS	South African Secret Service
SIGINT	Signals Intelligence
SNA	Social Network Analysis
SOCMINT	Social Media Intelligence
SSA	State Security Agency
SSC	State Security Committee
UDF	Union Defence Force
USSR	Union of Soviet Socialist Republics

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

"US policy makers, war fighters, and law enforcers now operate in a real-time worldwide decision and implementation environment. The rapidly changing circumstances in which they operate take on lives of their own, which are difficult or impossible to anticipate or predict. The only way to meet the continuously unpredictable challenges ahead of us is to match them with continuously unpredictable changes of our own. We must transform the intelligence community into a community that dynamically reinvents itself by continuously learning and adapting as the national security environment changes."
D Calvin Andrus[1] (2005)

1.1 Background, Motivation and Problem Statement

Over the past few decades the international landscape has become more complex, characterised by the fight against terrorism, ethnic conflicts within states, cyber threats, transnational crimes and global warming (Rathmell, 2002:87). This is taking place within the context of globalisation and an increased pace of technology development, especially technology related to communications and information (Perrons, 2004:169).

The pace of technological change[2] has been the most dramatic trend of the last half-century and is expected to continue for at least the next decade (Oxford Martin School, 2013:22). One of the most important technology changes is the emergence of the internet. According to Internet World Stats (2018), there were around 4 billion users worldwide in December 2017, compared to 738 million in 2000 (442%). This phenomenon has affected globalisation, democratisation, economic growth, and education and has brought with it an information revolution. Castells (2010a:xxxii) refers to information politics as a new form of politics that has emerged in the past two decades as a result of the information age, which is characterised by the revolution of information and communication technology (ICT). Within the internet domain, one of the most significant developments has been the emergence of social media.

Table 1: Number of social media users in 2018

SOCIAL MEDIA WEBSITE	NUMBER OF USERS GLOBALLY	NUMBER OF USERS SOUTH AFRICA
Facebook®	2 196 million	16 million

[1] Dr D Calvin Andrus, CIA's Directorate of Support.

[2] Computing power has been doubling almost every 18 months, virtually matching Gordon Moore's 1965 observation of 24 months, now widely referred to as Moore's Law. Gordon Moore (co-founder of Intel) at the time predicted that "the number of transistors on a chip will double approximately every two years". www.intel.com/content/www/us/en/silicon/moores-law-technology.html.

SOCIAL MEDIA WEBSITE	NUMBER OF USERS GLOBALLY	NUMBER OF USERS SOUTH AFRICA
YouTube™	1 900 million	8.74 million
Instagram™	1 000 million	3.8 million
Twitter®	336 million Twitter accounts	8 million Twitter accounts

Source: Statista, 2018; Vetromedia, 2018

The phenomenon of social media started in 1997 with SixDegrees.com and has since developed into a great number of communication tools, of which Facebook®, YouTube™, Twitter® and Instagram™ are but a few (see Table 1). Social media has significantly changed the way communication takes place. This communication tool is characterised by a global transmission and an increased level of use mainly because of its handiness, flexibility and cost-effectiveness. Social media connects like-minded people either to build friendships or to increase membership in support of a specific cause (Scott & Jacka, 2011:5). Many terrorist[3] and radical groups therefore use the internet and tools relating to the internet to communicate, distribute propaganda, recruit and train members (Bartlett & Miller, 2013:9; Schwab, 2016:77; Thomas, 2003:112; Thompson, 2011:167; Weimann, 2004:1).

It is exactly this application of social media that motivated Omand[4] *et al*. (2012a:804) to describe this phenomenon as a "disruptive technological development". They argue that new methods of communication, such as social media, necessitate a response from public institutions, including intelligence services. It is in this article that the authors first coined the term SOCMINT[5] to refer to intelligence derived from social media (Omand *et al*., 2012a:804). The authors highlight the following opportunities that SOCMINT offers:

- Crowd-source information: This refers to better flow of information from citizens to government agencies, with specific reference to emergencies (for example, the earthquake in Haiti).

[3] Bartlett and Miller (2013:9) point out that most known terrorist organisations had an online presence by 1999.

[4] Sir David Omand GCB was appointed in 2002 as the first UK Security and Intelligence Coordinator, responsible to the Prime Minister for the professional health of the intelligence community, the national counterterrorism strategy and "homeland security". He served for seven years on the Joint Intelligence Committee.

[5] In a follow-up article in 2013, Bartlett and Miller (2013:14) mention that SOCMINT is defined by its existence on a social media platform and not by the openness of the information and does not easily fit into the categories of open or secret intelligence.

- Research and understanding: Researching social media could lead to a better understanding of various issues relating to social interaction and behaviour (radicalisation).
- Near real-time situation awareness: Social media can assist in creating a picture of the unfolding of events (for example, the events during the Arab Spring).
- Insight into groups: Social media can assist in understanding political and radical groups suspected of illegal activities (Omand *et al*., 2012a:804–806).

The authors point out that although these opportunities merit granting SOCMINT a significant place within the national intelligence (NI) framework, there are, however, challenges that have to be addressed (Omand *et al.,* 2012a:802). These challenges are mainly concerned with public acceptability, especially as it relates to necessity[6] and legitimacy[7] (Omand *et al.,* 2012a:816). SOCMINT can involve either open or covert intelligence, and it is in relation to the ways in which the covert information is obtained that the question of privacy is raised (Omand *et al.,* 2012:807). The public must be assured that the intelligence activities related to SOCMINT effectively contribute to the public good in a non-threatening way. The authors conclude that if governments want to conduct SOCMINT, it should be within a framework of accountability and respect for human rights (Omand *et al*., 2012a:823).

Although Difesa (2012) did not refer to SOCMINT directly, he raises some key security consequences when utilising social media. These include the following:

- Information security: Social media websites may unintentionally jeopardise information security. These websites facilitate security risks such as privacy infringements, corporate espionage and the spread of malware (data loss and identity theft). Shullich (2011:1) indicates that any website that enables a visiting user to post content opens a window for an organisation to be harmed.
- Information dissemination: Social media is a new mode of communicating information (positive or negative) quickly and to a great number of people.
- Intelligence operations: Social media is used by individuals and organisations to collect information. This may strengthen the ability of governments to monitor the behaviour of citizens, but it can also strengthen the position of non-state actors.

6 Contributes towards public safety.
7 No harm to public good.

- Organisational capabilities: Social media is a powerful tool to organise people for a specific cause. What makes this even more powerful is the fact that social media is not restricted by geographical borders.

The global landscape is changing mainly as a result of the increased pace of technology development and informationalisation (Castells, 2010a:72; Castells, 2010b:72). Within the changing global environment, government policies and strategies to address threats related to new technologies are currently outpaced by the technology revolution (Carafano, 2011:74; Wiemann, 2004:1). This raises the question of how new technologies, and specifically social media (in the case of this study), should be addressed within the intelligence environment. An important point of departure would therefore be to conceptualise and understand intelligence to address the specific role and function of SOCMINT within the security environment.

From the literature study it is evident that there are various approaches to theory on intelligence, including positivism, realism and postmodernism. Positivism and realism are the two traditional views. Kahn's (2001:84–85) traditional positivist theory is built on three principles: the function of intelligence is to optimise one's resources; intelligence is an auxiliary and not the primary element in war; and intelligence defines the offensive. Kahn (2001:79) also defines intelligence in the broadest sense as "information". Phythian (2009:58) on the other hand supports structural realism and he is of the opinion that "structural realism already provides a theoretical explanation for certain key questions in intelligence studies". According to Phythian (2009:58), the following factors from structural realism relating to the international system explain the need for intelligence:

- great powers are the main actors in world politics;
- all states possess some offensive military capability;
- a state can never be certain about the intention of other states;
- the main goal of states is survival; and
- states are rational actors.

Another and relatively new approach is Rathmell's (2002:87) postmodern theory on intelligence. According to Rathmell (2002:87), "the concept of postmodern[8] intelligence may not by itself adequately characterise all facets of the contemporary intelligence environment,

[8] "Postmodernism refers to the emergence of new approaches towards knowledge and the processes of creating knowledge" (Rathmell, 2002:88).

the term does provide a valuable conceptual framework within which change can be managed and intelligence sources and methods can be adapted to a new era".

Despite the intelligence theories, it is very difficult to construct a definition for intelligence, since intelligence has different meanings for different people (Treverton *et al*., 2006:2). Most definitions of intelligence are based on Sherman Kent's[9] (1966:vii) explanation of the concept as "the knowledge which our highly placed civilian and military men must have to safeguard the national welfare". In addition, Kent (1966:ix) refers to the three "distinct things" intelligence practitioners refer to when they use the word intelligence:

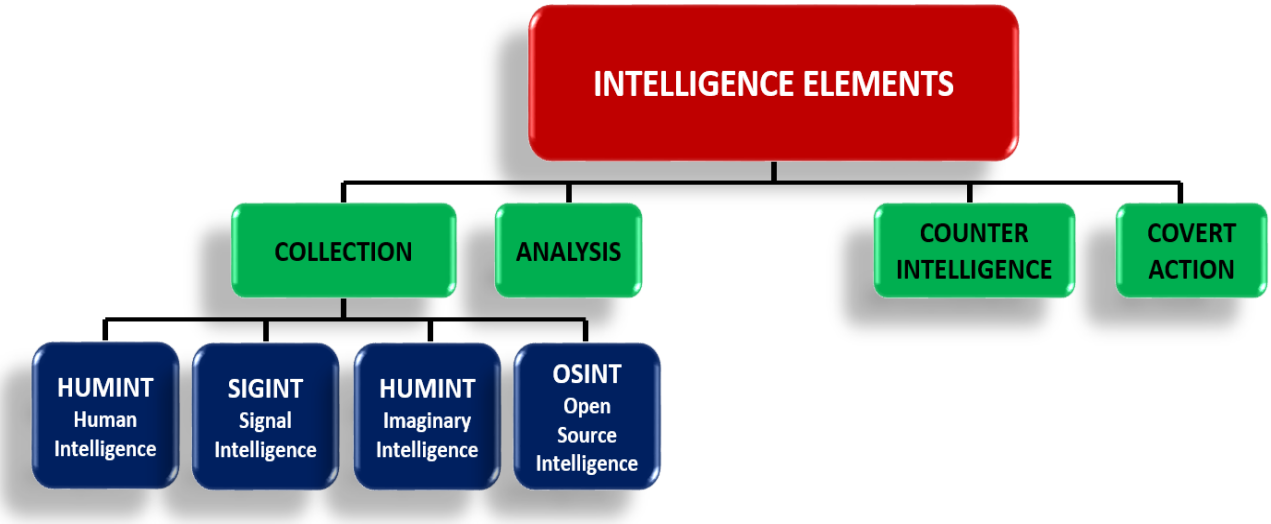
- knowledge – finished intelligence product;
- organisation – way in which intelligence services are organised; and
- activity – way intelligence services collect and analyse information.

The elements or functions of intelligence can be deduced from the definitions above. These include collection, analysis, counterintelligence and covert action (Gill & Phythian, 2006:62–101; Lowenthal, 2006:54–172; Shulsky & Schmitt, 2002:8) as depicted in Figure 1. Collection refers to the gathering of raw data through various means (human intelligence – HUMINT, signal intelligence – SIGINT, imagery intelligence – IMINT, open source intelligence – OSINT) (Lowenthal, 2006:59; Shulsky & Schmitt, 2002:8). The next important element is analysis. According to the Geneva Centre for the Democratic Control of Armed Forces (DCAF)[10] (2003:15), analysis is "the term used for the process of collation, analysis and evaluation of raw information and its transformation into intelligence". Counterintelligence is the national effort to counter and prevent foreign intelligence services from espionage, subversion and sabotage (DCAF, 2003:16). Covert collection is also an element of intelligence and is used by some countries to "influence political, military and economic conditions abroad" (DCAF, 2003:17). Within the South African intelligence context, the collection of information is focused on HUMINT, signal intelligence (interceptions) and OSINT. Intelligence collection from communication technology other than signal capabilities such as social media is limited and unstructured.

---

[9] Sherman Kent is referred to as the "father of intelligence analysis". His greatest contribution to the intelligence community was the development of a formal analytical "tradecraft" and method. His book, *Strategic Intelligence for American World Policy*, written in 1949 and reprinted (1966), was instrumental in formalising analytical tradecraft and methodologies. The CIA named its analysis training institute after Kent.

[10] The DCAF (a centre for security, development and the rule of law) is an international foundation established in 2000 on the initiative of the Swiss Confederation. The DCAF is based in Geneva and contributes to enhancing security sector governance through security sector reform.



Source: Own construct

Figure 1: Intelligence elements

Against this background it is important to note that intelligence is a dynamic science and it changes with its environment. The focus of intelligence has changed since the end of the Cold War in 1989. During the Cold War intelligence was principally geared to assist the military and to aid in the ideological and military struggle between East and West, represented by the United States of America (USA) and the Soviet Union. Countries aligned themselves along these lines and focused their security priorities accordingly (Johnson, 1999:6; Sheehan, 2000:329; Treverton, 2011:1). After the end of the Cold War the security focus changed and because of the borderless environment, the enemy is no longer state-bound. The focus has shifted to issues such as the proliferation of weapons of mass destruction, growth of ethnic nationalism and extremism, international terrorism and transnational crimes (Johnson, 1999:5). National security is no longer limited to a country's own borders, but has to consider a common global enemy.

Similarly, the South African intelligence service also experienced a major change after the end of Apartheid in 1994. The focus of intelligence during Apartheid was on liberation movements, including the African National Congress (ANC). After 1994 the focus of national security shifted to a wider range of threats related to both the South African state and society at large (O'Brien, 2011:10). The White Paper on Intelligence (1995) and the Constitution of the Republic of South Africa (1996) form the backbone of the new approach to security in general and intelligence in particular. According to Section 198 (a) of the Constitution of the Republic of South Africa (1996), "National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free

from fear and want and to seek a better life". Africa (2012:102–103) refers to the following three pillars of intelligence policy after apartheid:

- The philosophical underpinnings of the intelligence system, which include the norms and values to which the intelligence services should adhere as set out in the White Paper (1995) and the Constitution (1996);
- the practice of intelligence, which refers to what the intelligence services do and how they interpret their legal mandate; and
- the impact of intelligence on society, particularly on the ability of individuals to exercise their constitutional rights.

Intelligence has not only been influenced by global political and economic changes, but is also confronted with changes related to technology. Lawlor (2007:14) highlights the most important results of the communication technology revolution. Some of these include the following:

- The development of the personal computer (PC): In 1975 the IBM 5100 was the first commercially available portable computer. In 1981 IBM produced the first PC. According to a report by Nielsen (2012), there were 6 million PCs in South Africa by 2011.
- Invention of the World Wide Web in 1991: In South Africa the internet user base increased from 2.4 million in 2015 to 30.8 million in 2018, representing 60% of the South African population (We Are Social & Hootsuite, 2018).
- Fibre optics development: The ICT evolution has increased communication power through the progress in fibre optic development, allowing the expansion of bandwidth and increasing quality, as well as the capability of computing. The effortlessness of communicating has increased the volume of information that is being sent from one place to another. This has implications for individuals, organisations and governments (Perrons, 2004:169). South Africa is currently served by five submarine communication cables:[11] South Atlantic 2 (SAT-2); South Atlantic 3/West Africa Submarine Cable/South Africa Far East (SAT-3/WASC/SAFE); SEACOM; the East African Submarine Cable System (EASSy) and the West African Cable System (Many Possibilities, 2014). The Main One, the Africa Coast to Europe, the South Atlantic Express (SAex), the BRICS Cable and WASACE Cable have been proposed or are under construction and are not operational yet (Many Possibilities, 2014).

[11] A submarine communication cable is a cable laid on the sea bed between land-based stations in order to carry telecommunication signals. Modern cables use optical fibre to carry digital data.

- Mobile phones, digital cameras: In January 2018 there were 87.07 million mobile connections in South Africa (We Are Social & Hootsuite, 2018).
- Active social media accounts: 18 million active social media accounts in January 2015 (We Are Social & Hootsuite, 2018).

Technology, specifically digital technology, has transformed the communication sector in such a way that global processes are taking place in a borderless environment. This has made the regulation and management of information very difficult (Castells 2010a:xxxii; Perrons, 2004:169; Shulsky & Schmitt, 2002:141). In spite of the research on social media conducted in the public, private and academic spheres, it is not yet an academic discipline or a distinctive intelligence tradecraft (Bartlett & Miller, 2013:3). The National Security Training Institute (NSTi, 2012:1) in the USA has indicated that communication technology, especially the internet and social media, are continuously growing and changing, but national security has lagged behind. Likewise, the current South African intelligence environment does not accommodate and formally recognise SOCMINT as part of the intelligence cycle, process or source of information. However, the negative application of social media, its implications for national security and the vast information it creates, merits an intelligence perspective on the topic. SOCMINT necessitates the design of a framework to guide the use of social media to the advantage of security sectors within the government. It is against this background that this study examines social media to place it within the South African intelligence context.

Noting the challenges new technologies pose to intelligence services, the following research statement underpins this study: *This study systematically investigates intelligence and social media to develop a theoretical and strategic framework that incorporates SOCMINT in the intelligence environment, explaining its role within the intelligence cycle, its application as a source of information and the threats and opportunities related to it.*

1.2 Central Theoretical Statement

Technological development over the past three decades has influenced every aspect of society and has played a key role in the production, dissemination and access of information. The extensive change in technology and the particular role of social media are creating certain opportunities, but they also pose threats to intelligence (Matey, 2005:15). *Social media is a new source of intelligence that creates threats and provides opportunities for the intelligence community in South Africa. It is therefore important to develop a theoretical and strategic framework that includes SOCMINT to mandate and guide the*

application of this source of intelligence within the intelligence environment. In order to address the research problem successfully, a cursory literature study follows below.

1.3 Literature Review

The main goal of a literature study is to give a clear understanding of an identified problem (De Vos *et al.*, 2011:134). Mouton (2011:87) refers to a literature review as "a body of scholarship, because your interest is not merely in literature but in the body of accumulated scholarship". Mouton (2011:87) underlines the importance of an extensive literature review by stating that the aims of a literature review are:

- to ensure that there is no replication;
- to learn the most recent theories on the subject;
- to ascertain the most widely accepted empirical findings within the field;
- to identify available instrumentation that has proven validity and reliability; and
- to find most widely accepted definitions of key concepts in the field.

The literature review for this study is divided into three parts, namely the theoretical conceptualisation of intelligence within the field of security studies, a conceptualisation of social media internationally, and the contextualisation of social media within the South African intelligence environment. For this study the literature that has been reviewed includes books, journals, internet articles, mini- and PhD theses, and South African legislation.

Intelligence belongs within the political science field as a sub-discipline of security studies, which is in turn a sub-discipline of international relations. It is therefore of great importance to contextualise security studies in an effort to understand intelligence and how it affects global political issues. The discussion first focuses on political science and international relations by considering sources such as *A comparative introduction to political science* (Jackson & Jackson, 1997); *An introduction to political science: comparative and world politics* (Jackson & Jackson, 2003); *Politics* (Heywood, 2002) and *Introduction to IR: Theories and Approaches* (Jackson & Sørensen, 2010). With regard to security studies, sources such as *Security Studies: An introduction* (Williams, 2008); *Security, strategy and critical theory* (Jones, 1999); *The evolution of International Security Studies* (Buzan & Hansen, 2009); *The concept of security* (Baldwin, 1997); *People, states and fear: the national security problem in international relations* (Buzan, 1983); *What is security?*

(Rothschild, 1995); *Redefining security* (Ullman, 1983); *National security as an ambiguous symbol* (Wolfers, 1952); *Theory of world security* (Booth, 2007) and the *Role of security and strategic studies within international relations studies* (Suchý, 2003) are examined to provide an initial overview of the key theoretical approaches, central concepts and significant themes within this field.

In order to understand intelligence theory, helpful sources include *A historical theory of intelligence* (Kahn, 2001); *Towards postmodern intelligence* (Rathmell, 2002); *Sketches for a theory of strategic intelligence* (Johnson, 1999); *Defending adaptive realism: intelligence theory comes of age* (Sims, 2009) and *Strategic intelligence for American world policy* (Kent, 1966). These sources provide the theoretical underpinnings of the conceptualisation of intelligence. These insights are amplified by the collection of essays in *Intelligence theory: Key questions and debates* (Gill *et al*., 2009); *The study of intelligence in theory and in practice* (Scott & Jackson, 2004) and *Towards a theory of intelligence* (Treverton *et al.*, 2006).

A further collection of sources are consulted to define intelligence and analyse the elements and functions of intelligence. These sources are *Strategic intelligence for American world policy* (Kent 1966); *Intelligence from secrets to policies* (Lowenthal, 2006); *Intelligence in an insecure world* (Gill & Phythian, 2006); *Intelligence and National Security: the secret world of spies* (Johnson & Wirtz, 2011); *What is intelligence? Information for decision makers* (Sims, 2009); *What is intelligence? Secrets and competition among states* (Shulsky, 1995); *A new definition of intelligence* (Breakspear, 2013); *Wanted: A definition of intelligence* (Warner, 2002); *Intelligence for the twenty-first century* (Dupont, 2003) and *Silent warfare: understanding the world of intelligence* (Shulsky & Schmitt, 2002).

The study also considers intelligence within the South African context. In South Africa the field of intelligence is relatively new and therefore research on this topic is limited, especially after the end of Apartheid. There are, however, sufficient sources to give a clear indication of how intelligence has evolved since 1949 and how it is applied within the South African context. Relevant sources include *The policy evolution of the South African intelligence evolution* (Africa, 2012); *The South African intelligence services* (O'Brien, 2011); *The white paper on Intelligence* (1995) and *The Constitution of the Republic of South Africa* (1996).

As social media is a fairly recent phenomenon and SOCMINT is a new area of interest, literature concerning this issue is limited globally and within the South African context. The technology revolution, and specifically the social media aspect, is addressed by viewing

sources such as *Introducing social media intelligence – SOCMINT* (Omand *et al*., 2012); *The power of identity* (Castells, 2010); *Auditing social media* (Scott & Jacka, 2011); *Using social media for global security* (Gupta, 2013); *Social media bible* (Safko, 2012); *The age of globalisation: Impact of information technology on global business strategies* (Lawlor, 2007); *Radicalisation and the use of social media* (Thompson, 2011); *How modern terrorism uses the internet* (Weimann, 2004); *Mastering the art of Wiki* (Carafano, 2011); *Impact of social media on national security* (Montagnese, 2012) and *Terrorist use of the internet: information operations in cyber space* (Theohary & Rollins, 2011).

In an effort to address the research statement, the following research questions guide the research:

1.4 Research Questions

Considering the research topic and this study's research statement above, the following questions are addressed throughout the study:

- The primary research question of this study is: What threats and opportunities does social media hold for national security, and based on a detailed evaluation of the current intelligence theories, how can SOCMINT be included in a strategic framework for the South African security environment?

Several secondary questions arise from the primary research question:

- What are the current key theoretical approaches, central concepts and significant themes within the field of security studies and how do they relate to intelligence?
- What are the prevailing key theoretical approaches to intelligence with specific reference to the following topics:
  - theories of intelligence;
  - theories for intelligence;
  - key concepts of intelligence;
  - definitions of intelligence;
  - elements or functions of intelligence; and
  - intelligence and oversight?

- How has the changing global environment in general and communication technology in particular influenced intelligence since the end of the Cold War with respect to its mandate, application and functions?
- What is the South African approach to intelligence and how has this approach changed since the end of the Cold War and the end of Apartheid, with specific reference to the following matters:
  - definition and concepts;
  - elements or functions;
  - intelligence and oversight.
- What is social media and what are the threats to national security and opportunities for intelligence?
- As SOCMINT is a new phenomenon and its application poses threats and opportunities to national security in general and intelligence in particular, how can SOCMINT be incorporated, applied and managed within the South African intelligence environment?

1.5 Research Objectives

The following research objectives are central to addressing the research question. The primary research objective is:

- To investigate the threats and opportunities related to social media, and based on a detailed evaluation of the current intelligence theories, to incorporate SOCMINT within a strategic framework for the security environment.

The pursuit of the primary research objective is facilitated by the following secondary research objectives:

- Reconstructing the key theoretical approaches, central concepts and significant themes within the field of security studies and explaining how they relate to the intelligence area of study.
- Constructing the prevailing key theoretical approaches to intelligence with specific reference to the following topics:
  - explaining the various theories of intelligence;
  - explaining the various theories for intelligence;
  - explaining key concepts of intelligence;
  - defining intelligence as knowledge, activity and organisation;

    - explaining the elements or functions of intelligence; and
    - explaining the role of oversight within the intelligence environment.
- Studying the shifting global environment and explaining how the changing communication technology has influenced intelligence since the end of the Cold War with respect to its mandate, application and functions.
- Examining the approach to and the development of intelligence in South Africa since the end of the Cold War and Apartheid, with specific reference to the following matters:
    - defining intelligence and explaining concepts relating to intelligence;
    - defining and explaining the elements or functions of intelligence; and
    - explaining the role of oversight within the intelligence environment.
- Studying social media and identifying the threats and opportunities to national security and how these can be applied within the intelligence environment.
- As SOCMINT is a new phenomenon and its application poses threats and opportunities to national security in general and intelligence in particular, motivating how SOCMINT should be incorporated, applied and managed within the South African intelligence environment.

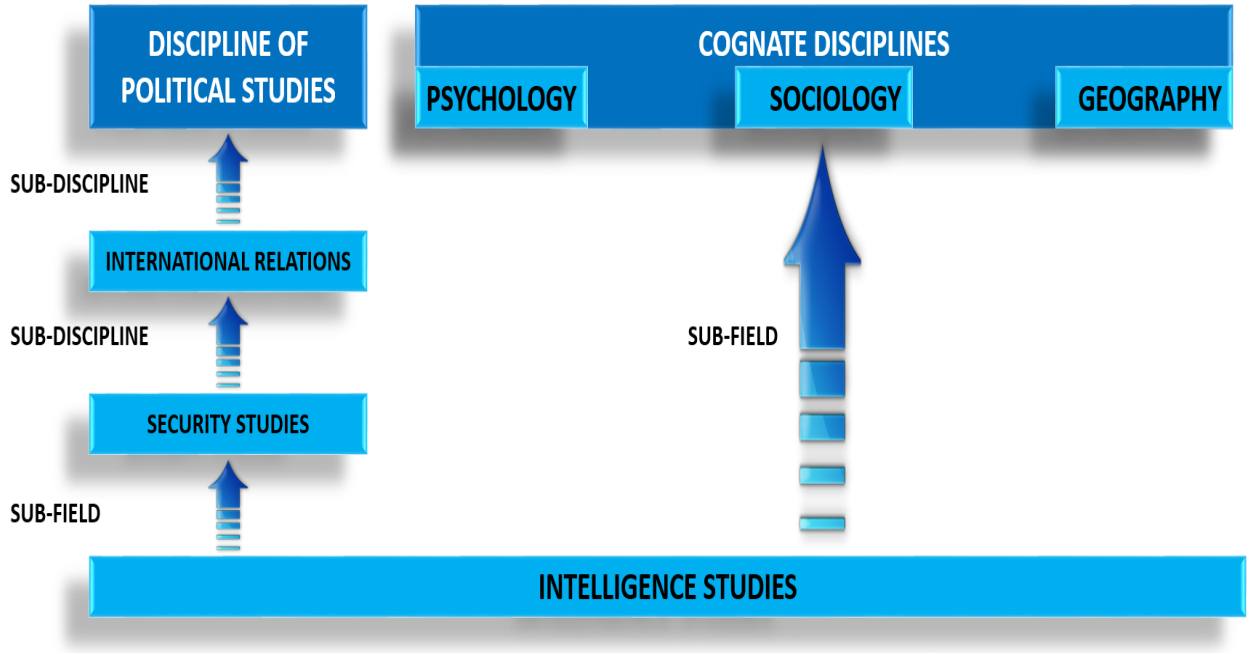
1.6 Methodology

The study opted for a qualitative research methodology, focusing on an in-depth literature study as explained above. Qualitative research involves studying characteristics or qualities that cannot be reduced to numerical values (Leedy & Ormrod, 2014:97). The aim of a qualitative study is to analyse the intricacies of a particular phenomenon (social media in the case of this study) to explain, interpret and describe the meaning and effects of this occurrence (Leedy & Ormrod, 2014:97–98; Berg, 2001:3). In this case, qualitative research was used to study and understand the new phenomenon of SOCMINT as a tool for intelligence collection.

Existing literature was examined as indicated in the cursory literature review included in this chapter. Since the study employed only existing overt literature and sources, no empirical data were gathered. No fieldwork was therefore conducted, and the study has limited ethical implications, if any.

The research design combines descriptive, explanatory and exploratory approaches. In an effort to understand intelligence, this study starts off with an exploratory analysis of its roots within the various academic fields. The relationship with the various disciplines is illustrated

in Figure 2. Although intelligence studies has its main origins within the political science domain, it does have links to cognate disciplines such as psychology, sociology and geography.



Source: Own construct

Figure 2: Roots of intelligence studies

As far as the study field is concerned, Kahn (2001:79) observed in 2001 (before 9/11) that although "intelligence has been an academic discipline for almost half a century" no theory of intelligence has been advanced. However, since 2001 the theory of intelligence has attracted more attention from various scholars (Phythian, 2009:54). According to Gill *et al*. (2009:1), the recent intelligence failures (specifically in the case of 9/11 and misidentification of weapons of mass destruction in Iraq) have raised theoretical thinking on intelligence, in particular questions about the efficiency of intelligence. A preliminary examination of intelligence theories shows several different approaches to the theory of intelligence. The approach within the field of intelligence studies is leaning towards realism. However, this study also explores the postmodern approach, mainly because it "provides a conceptual framework within which change can be managed and intelligence sources and methods can be adapted to a new era" (Rathmell, 2002:88).

The study explores, explains and evaluates social media to understand this new phenomenon. SOCMINT is explored, assessed and evaluated against this background as part of an intelligence collection environment. The goal of the evaluation is to understand

and conceptualise the threats and opportunities that SOCMINT holds for the intelligence environment and to create a strategic framework that includes this new phenomenon. The study uses deductive reasoning to create a South African intelligence framework to include the new phenomenon of SOCMINT as a tool for intelligence collection.
The contribution of this study is explained against this background.

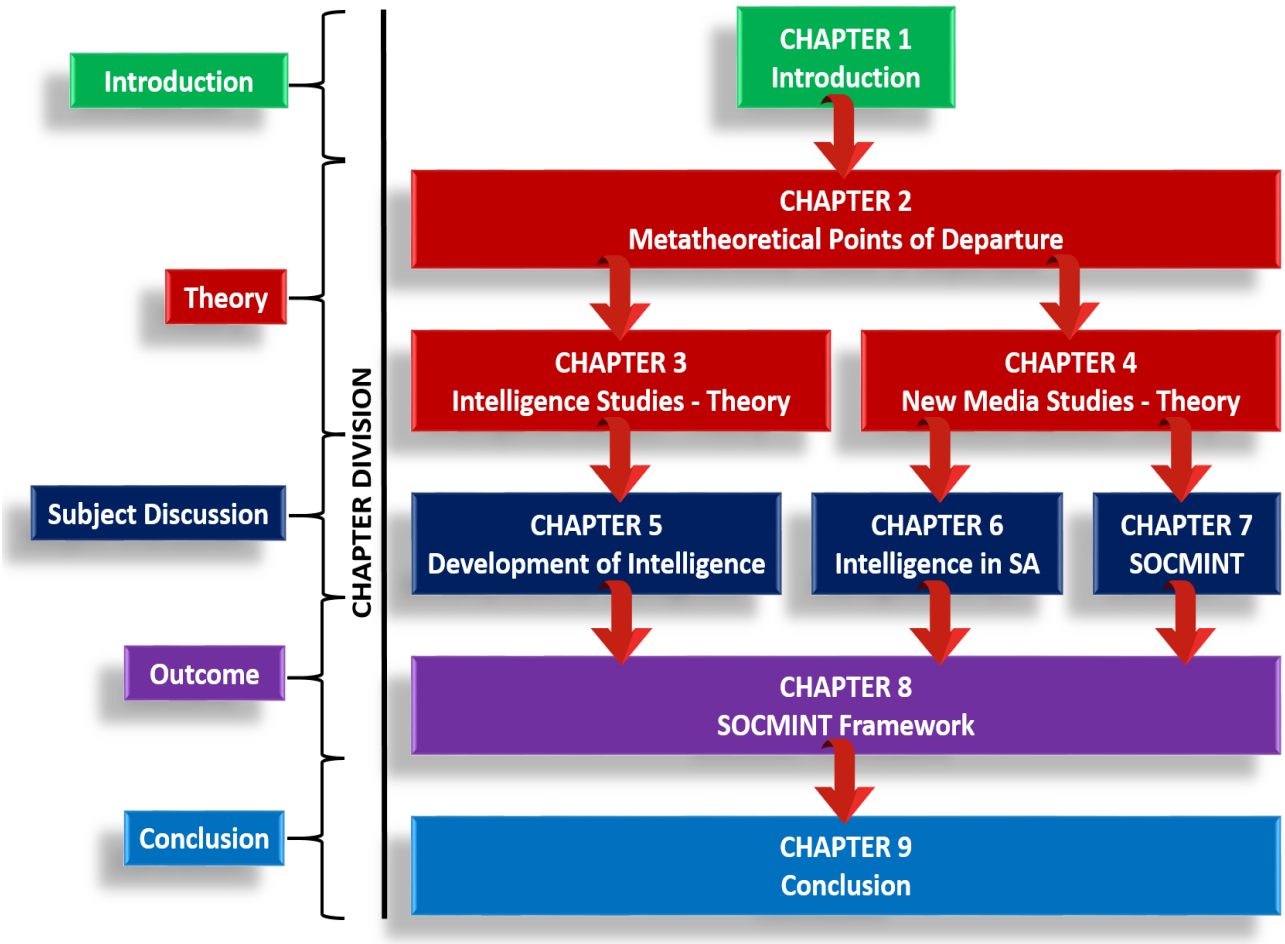
1.7 Contribution

"Intelligence, if we understand it, might someday be more clearly a force of good. If intelligence is ever to be a force for good, then it must be studied. We must bet that if we remain ignorant of it, intelligence will certainly be a force for ill" (Warner, 2009:30). This study is an attempt to understand social media and to incorporate SOCMINT in the South African intelligence environment to use it as "a force of good".

The debate on social media and SOCMINT is still in its infancy and further research is needed to understand how social media can be exploited for intelligence purposes. Until now no study has been done to explain the threats and opportunities of SOCMINT within the South African intelligence environment. The contribution of this study lies in the fact that it advances SOCMINT as an important source of intelligence and develops a strategic framework that will place it within the environment of the South African intelligence collection process. Such a study is timely and urgent, because the rapid pace of technology development is changing the communication landscape, but national security policies are not keeping up with these technology changes and their consequences.

1.8 Chapter Division

The chapter division is depicted in Figure 3 below, followed by a detailed discussion.



Source: Own construct

Figure 3: Chapter division

Chapter 1: Introduction

Chapter 1 serves as an introduction to the study. This chapter provides a brief overview of the structure of the study and its objectives and methods. Intelligence and SOCMINT are contextualised, based on which a problem statement, research questions and research objectives are derived. The methodology that was used to achieve the goals is discussed, as well as a brief outline of the contribution of the study. The introductory chapter concludes here by specifying the chapter division and briefly highlighting the content of each chapter.
The following eight chapters will complete this study:

Chapter 2: Metatheoretical points of departure

The main focus of this chapter is to construct a metatheoretical model as a basis for this study. The chapter starts off with an explanation of the philosophy of research, followed by a detailed discussion of social science research and its components. These components include pre-scientific consciousness, scientific knowledge, discipline, tradition, paradigm,

conceptual frameworks and finally definitions and concepts. The chapter concludes with a conceptual framework for understanding SOCMINT.

Chapter 3: Intelligence studies: metatheoretical, theoretical and conceptual orientation

Chapter 3 analyses the origins of the field of intelligence studies. The chapter begins by explaining the academic foundation and development of intelligence studies. The origin, definition, concepts and theories related to political science, international relations and security studies are first discussed. Theories on and approaches to intelligence studies follow. This section includes a discussion on the changing security context. In addition, the chapter clarifies and discusses the central concepts underpinning the field of intelligence. The chapter concludes with the conceptualisation model of intelligence.

Chapter 4: New media studies: metatheoretical, theoretical and conceptual orientation

Chapter 4 emphasises the metatheoretical and theoretical point of departure for new media studies. The chapter focuses on the academic foundation of new media studies within the discipline of communication studies. The traditions, paradigms, conceptual frameworks and concepts relevant to social media are highlighted to compile a metatheoretical framework to understand SOCMINT.

Chapter 5: The evolution of the intelligence profession and the role of technology

Chapter 5 examines the evolution and development of intelligence. Although this chapter commences by examining espionage as the root of modern day intelligence, greater emphasis is placed on developments since World War I and II, the Cold War and post-Cold War period, as these time periods link up with developments in the technology field. The chapter then continues to examine the evolution of technology in general and communication technology in particular and explains how this has given rise to the information revolution.

Chapter 6: The history and development of intelligence within the South African context

Chapter 6 analyses intelligence within the South African context. The chapter explains and defines intelligence within the South African environment and addresses major historic developments since 1948. Greater emphasis is placed on the development of intelligence since the end of Apartheid in 1994 and on how the focus has shifted to include the South African state and society.

Chapter 7: SOCMINT and its global application

Chapter 7 starts with an explanation of the internet and social media, and the history of this new phenomenon. The chapter then focuses on a detailed study of how social media is applied within the global communication environment and explains how this occurrence poses threats and opportunities to national security. With this in mind, the chapter then explores SOCMINT as a new source of intelligence collection by defining SOCMINT. The chapter explains the applications within the intelligence environment and investigates how information can be extracted for intelligence purposes.

Chapter 8: A framework for SOCMINT in the South African context

Chapter 7 makes it quite apparent that there is a lack of information on SOCMINT and its application within the intelligence environment. Chapter 8 focuses on this new phenomenon within the South African environment. The chapter begins with the social media landscape within South Africa. This forms the basis of the subsequent discussion on SOCMINT application within South Africa. This chapter furthermore develops a strategic framework that includes SOCMINT within the South African intelligence environment. Additionally, the chapter addresses SOCMINT and the issue of oversight, responsibility and accountability within South Africa. The chapter concludes with findings and recommendations.

Chapter 9: Conclusion

The study concludes with a summary and integration of preceding chapters.

CHAPTER 2: METATHEORETICAL POINTS OF DEPARTURE

"The highest quality power comes from the application of knowledge."
Alvin Toffler, 1990

2.1 Introduction

Toffler (1990:12) is of the opinion that power entails three aspects: violence, wealth and knowledge, with the latter being the most important because of its efficiency and versatility. He furthermore states that "knowledge is the most democratic source of power" (Toffler, 1990:19). Today we live in a borderless world of information overload and the identification of the correct information from which to gain knowledge, and therefore power is of utmost importance. This power is geared towards political independence in a world filled with new security issues as a result of the increase in information and constantly evolving technology. The information age created by the technology revolution has also affected the global intelligence environment, providing both opportunities (access to more information) and threats (terrorism). However, the intelligence community has not fully embraced the changed environment and modifications to the way intelligence is being conducted have received little attention. Why is it so important to stay in touch with changes and developments, especially technological developments? The answer to this vital question can be found in the mandate of the intelligence services. This mandate is the provision of information to the decision maker to assist with policy formulation on issues related to national security. It is imperative to provide timely and relevant information. Recent technological developments have increased the access to and availability of information and, as intelligence is in the knowledge and information business, it is imperative that intelligence services stay abreast of these changes to provide the decision makers with timely and relevant information.

As indicated in the first chapter, this study aims to provide a framework for SOCMINT within the South African intelligence context. In order to achieve this objective and to contribute to the knowledge base, it is imperative that the metatheoretical departure points that support this framework be outlined and discussed in detail.

There is currently no agreement on a clear definition of the concept of metatheory. This is illustrated in Steven Wallis's paper *Towards a science of metatheory* (2010) where he presents 20 different definitions for metatheory. A few of these definitions are mentioned to

indicate the importance of metatheory and to clarify the significance of a well-defined metatheoretical framework.

In its simplest form, metatheory is “theory about theory”. Abrams and Hogg (2004:100) are more descriptive in their definition: “A metatheory should provide an alternative framework for asking particular questions, not a complete explanation for all phenomena. A strong metatheory helps to put the body parts together in a meaningful structure and then to theorise links between those parts. In addition, identifying the metatheory behind a particular theory helps reveal potentially interesting and useful links to other theories.” Anchin (2008:235) supports Abrams and Hogg’s (2004:100) view and argues that “unifying knowledge in any field of endeavour requires metatheory comprising a conceptual scaffolding that is sufficiently broad to encompass all of the knowledge domains distinctly pertinent to the field under consideration, that can serve as a coherent framework for systematically interrelating the essential knowledge elements within and among those domains, and that extends conceptual tendrils into the fields of study”.

From these definitions, it is clear that a metatheoretical framework is of great importance, as it shapes the study by providing it with an outline and a foundation on which the research is conducted. Furthermore, a metatheoretical framework is vital to both the researcher and the reader: to the researcher, it provides a guideline for conducting the research and to the reader, it offers a better understanding of the study. For the purposes of this study, a metatheory is defined as the theoretical assumptions that ground the study, guide the researcher in the research process and provides the reader with an understanding of the issue at hand. Metatheory for this study is imperative for various reasons. In the first place, metatheory will provide a framework to understand the SOCMINT phenomenon and to guide the researcher in the research endeavours. Secondly, this study is a combination of two academic fields (as is explained later): intelligence studies and new media studies. In order to reach the goals as set out in Chapter 1, the metatheory for both these fields should be examined. This enables the development of a combined metatheory to explain and ground SOCMINT. Furthermore, it contributes to the theory base of intelligence studies, which is currently very limited. Finally, metatheory also provides and explains links with other fields of study, in the case of this study the links with new media studies.

With this explanation of metatheory as background, it is important to once again highlight that the main aim of this study is to develop a strategic framework that incorporates SOCMINT and its functions into the intelligence environment for application as a new source of information. The key focus of this chapter is to provide the metatheoretical

conceptualisation or agenda to compile the SOCMINT framework, and furthermore, to contribute to the scientific knowledge base.

This chapter focuses on the following aspects:

- The philosophy of research: This section is a brief orientation with respect to the philosophy of research.
- Social science research: This section explains how this study fits into the framework of the social sciences. The discussion highlights the dimensions of social science research (sociological, ontological, teleological, epistemological and methodological).
- Components of social research: These components include the pre-scientific consciousness, scientific knowledge, discipline, tradition, paradigm, conceptual frameworks, and finally, definitions and concepts. Each of these components is discussed in detail.
- A conceptual framework to understand SOCMINT: This chapter concludes with the construction of a conceptual framework for understanding SOCMINT by applying the components identified in social science research.

The conceptual framework guides the research process and helps the reader to understand the study. The next section begins with a brief discussion of the philosophy of research in general and social science in particular.

2.2 The philosophy of research

Research is an important part of developing civilisation and it started in the early ages. The main aim of research is to expand knowledge. According to Babbie (2008:7), everybody has a desire to learn more about something, and this usually comes about through experience, investigation, tradition and authority, which he terms “second-hand knowledge”. However, to contribute to the scientific knowledge base we need to focus on scientific research. By doing research, we are developing and increasing scientific knowledge in a particular field (Saunders *et al*., 2012:127).

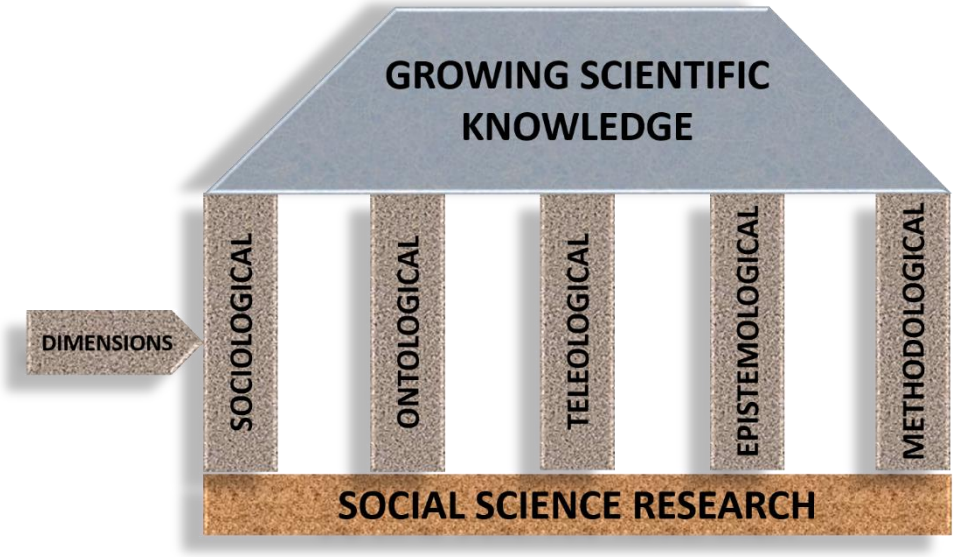
The first and most important aspect of any research is the philosophy of research. According to the Concise Oxford English Dictionary (2004:1077), philosophy is “the study of the fundamental nature of knowledge, reality and existence, a theory or attitude that guides one’s behaviour”. This point is amplified by Williams and May (2003:4), who are of the

opinion that research philosophy is concerned with abstract questions related to the development of knowledge and the nature of that knowledge, how the world is observed and how we can best come to understand it. Once there is an understanding of the philosophy behind the research, the researcher is in a better position to examine the social phenomenon. Therefore, philosophy is an activity of thought that offers a foundation for every scientific discipline and creates the framework to do scientific research. In the case of this study, the philosophies at the basis of intelligence studies and new media studies frame the study and the research into SOCMINT.

When attempting to conceptualise the philosophy of social science research, various aspects should be taken into account. These aspects include the fields of ontology, epistemology and methodology (instruments used to obtain the knowledge), which are the starting points for any scientific research. However, Burrell (2005:1) also includes human nature as a fourth assumption and Mouton and Marais (1996:8) include “sociological and ideological dimensions” in their model of “dimensions of social science research”. As highlighted previously, the philosophy of research forms the basis for social science research and it is subsequently discussed in detail in the following section.

2.3 Social science research

This study originates within the field of political science and belongs to the domain of social sciences. In an effort to enhance the metatheoretical departure points for this study, the discussion first reflects on and unpacks the concept of social science research. According to Mouton and Marais (1996:7), social science research is “collaborative activity in which social reality is studied objectively with the aim of gaining a valid understanding of it”. Based on this definition, the authors propose five dimensions of social science research that are equally important for successfully conducting research in the social science domain (Mouton & Marais, 1996:8-15). These dimensions are depicted in Figure 4 as pillars for social science research that are important in growing scientific knowledge. All these dimensions work together towards growing the body of knowledge.



Source: Adapted from Mouton & Marais, 1996

Figure 4: Dimensions of social science research

The first dimension (Mouton & Marais, 1996:8) is the sociological dimension, which refers to interaction and cooperation among researchers. Although this idea of collaboration is common practice in the research environment today, this was not always the case. During the Renaissance, scientific research was viewed as secret and the exclusive property of the researcher. It was not until the 17th century that this practice changed and cooperation among scientists was promoted (Mouton & Marais, 1996:8).

The second dimension is the ontological dimension (Mouton & Marais, 1996:11). Ontology is a branch of metaphysics dealing with the nature or science of being (Concise Oxford English Dictionary, 2004:1000; Hay, 2006:80; Marsh & Furlong, 2002:18; Mouton & Marais, 1996:11). The word being is derived from the Greek word "existence". Ontology deals with questions such as whether there is a "real world out there" that is independent of our knowledge of it (foundationalist) and whether we influence the "world out there" by socially constructing it (anti-foundationalist) (Marsh & Furlong, 2002:18). Blaikie (1993:6–7) takes it further and argues that objects can be real or ideal and researchers give meaning to objects through their research and findings. There are various approaches to or theories on ontology. According to Saunders *et al*. (2012:131), there are two distinct theories on ontology, inter alia objectivism and subjectivism. Objectivism implies that in reality, social entities exist independently and externally from social actors (foundationalist). Social actors have no influence over the social entities. In contrast, subjectivism suggests that social

actors have a direct impact on social phenomena in that these phenomena are created from the perceptions and actions of social actors (anti-foundationalist).

It is clear that although various definitions of ontology exist, in essence, it has to do with reality and how we perceive it. How we view reality depends on our value systems, which have an important influence on the research we decide to pursue and the way in which we pursue it (Saunders *et al.*, 2012:127). According to Mouton and Marais (1996:11), in the case of social sciences, the reality is the research domain. This study's research domain, reality or phenomenon is social media. This world or phenomenon is being constructed or created by the social actors (anti-foundationalist ontology). Through the use of social media, social actors are creating another world and the result of this creation is SOCMINT, which needs to be understood to fully comprehend its impact on national security.

Mouton and Marais (1996:13) refer to teleology[12] or ideology as the third dimension of social science research. This dimension highlights the fact that scientific research is "goal-directed" and its main focus is to either gain a theoretical understanding of the specific social phenomenon or practical knowledge on how to adjust human actions and behaviour. With regard to this study, the main goal is to gain a better understanding of SOCMINT and to create a strategic framework for the national security environment within the South African context. The use of social media is investigated and analysed as a starting point to appreciate its implications and applications for national security.

The fourth dimension is epistemology and Mouton and Marais (1996:14) regard it as a crucial dimension in the practice of social science, mainly because of the importance of the quest for truthful knowledge. The Concise Oxford English Dictionary (2004:480) describes epistemology as the "theory of knowledge, especially with regard to its methods, validity and scope and the distinction between justified belief and opinion". The word epistemology takes its modern meaning from 19th century Greek and is derived from *episteme*, which is knowledge, and *logos*, which is to study. Epistemology is the theory or science of knowledge (Blaikie, 1993:18; Hay, 2006:83; Henn *et al*., 2006:10) and is one of the fundamental parts of philosophy. According to Klein (2005:224), it is "concerned with the nature, source and limits of knowledge". He also argues that "the central question to epistemology is: what must be added to true beliefs to convert them into knowledge?" Saunders *et al*. (2012:132) add another element and explain that epistemology is "concerned with what is acceptable knowledge". However, Mouton and Marais (1996:15) are of the opinion that unlike the

[12] "Telos" is the Greek word for "goal".

natural sciences, complete certainty in the social sciences is unachievable mainly because we are dealing with humans. The aim of research in the social sciences should be to arrive at findings as close as possible to reality. Similar to ontology, the field of epistemology also has different approaches relating to this science. These approaches include positivism, realism, direct realism, critical realism and interpretivism (Blaikie, 2010:94–95; Terre Blanche *et al*., 2012:6). The most common classification is that of positivists and interpretivists (Marsh & Furlong, 2002:19).

From this brief discussion one can extrapolate that epistemology in its simplest form is a science of knowledge, concerned with acceptable knowledge. For the purposes of this study, epistemology is the science of knowledge in relation to intelligence studies and new media studies. The approach relevant to this study is the interpretivist approach, the main reason being that the interpretivists gain an understanding of social behaviour through observation and interpretation of the phenomena to attach meaning. This study observes the social phenomenon of social media in an effort to understand its behaviour and the implications for intelligence and national security. The knowledge gained has assisted in compiling a framework for the application of SOCMINT within the security environment in South Africa.

The final aspect in the Mouton and Marais (1996:15) explanation of social science research is the methodological dimension, which is concerned with the "how" of research. According to Kaufmann (1958:230), "the logic of science (which is the methodology) is the theory of correct scientific decisions". The Concise Oxford English Dictionary (2004:898) explains methodology as "a system of methods used in a particular area of study or activity". The term has its origins in early 19th century Latin *methodologia*. Methodology refers to the analytical strategy and research design supporting a study. Within the social sciences, qualitative and quantitative methods of research are widely used. Researchers have to make decisions on theories, models, hypotheses, measuring instruments and the method to be used in the analyses of data. The main aim of the methodological investigation is to eliminate incorrect decisions in an effort to obtain the most valid and objective outcomes (Mouton & Marais, 1996:16). Two of the main differences between qualitative and quantitative methods are the information and techniques used as a basis for assumptions (Terre Blanche *et al*., 2012:47). Quantitative methods gather information and data in the form of numbers and apply statistical analyses to draw conclusions. Qualitative methods observe a phenomenon and document the observation, using the spoken and written language to collect data. The decision on which method to use will depend on the main goal of the study. Qualitative research is more appropriate when researching or exploring a subject not well known or to grasp the meaning, motives or patterns within the social

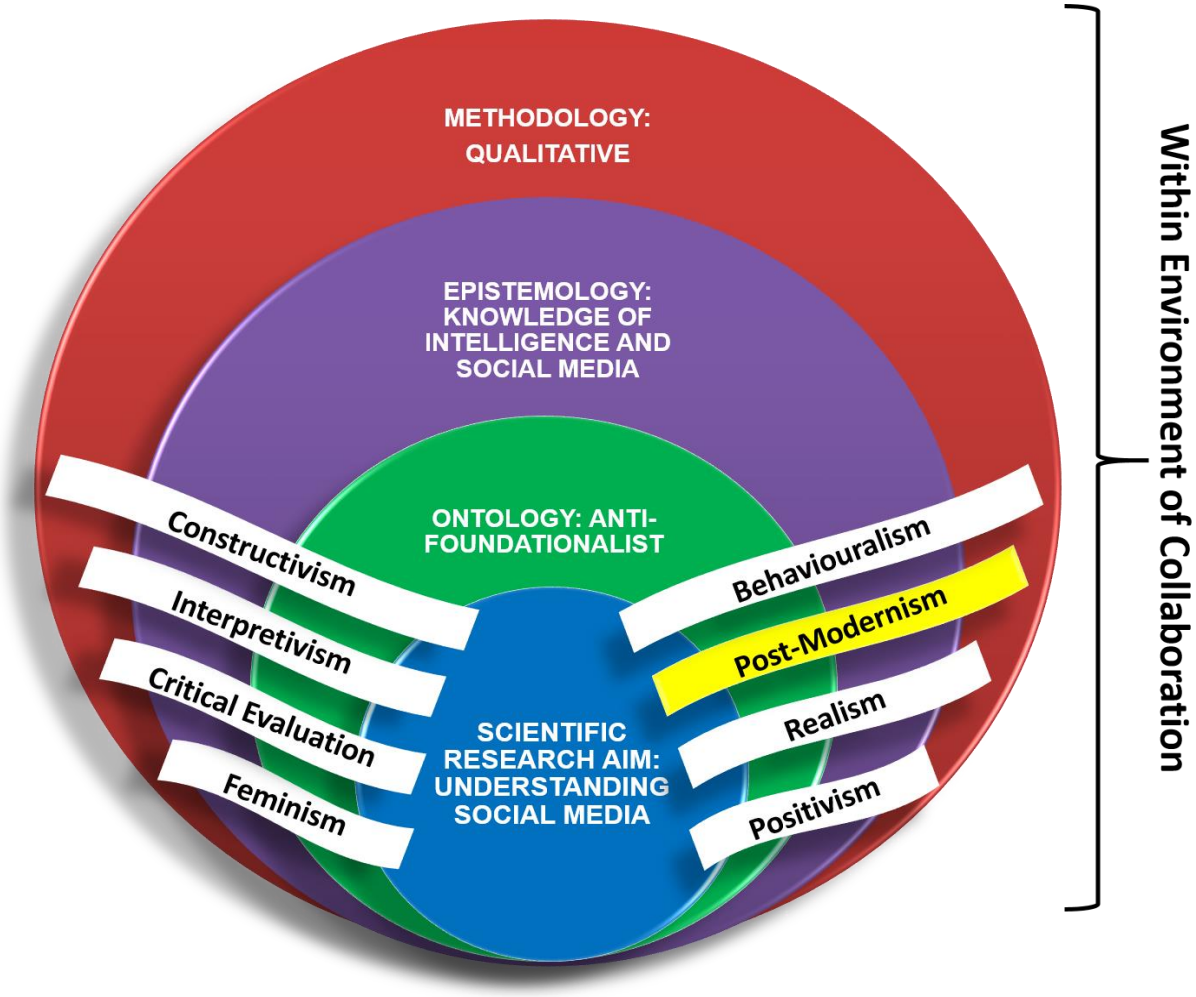
environment, such as with the use of social media. Quantitative research is better suited when testing theories with hypotheses or comparing data in a systematic way.

This study focuses on a qualitative methodology and applies a comprehensive literature review to reach the research objectives set out in Chapter 1. This method aids the investigation of the patterns and implications of social media for the intelligence environment and the compilation of a framework to incorporate SOCMINT within the intelligence structure.

In examining social science research, it is clear that there are various approaches. Social scientists had to look into different ways of approaching and researching phenomena in this field due to difficulties faced by social sciences in relation to the measurability of subject matter (De Vos *et al*., 2011:5). Different social research experts give credence to different approaches and there is no agreement on which approach is the best. De Vos *et al.* (2011:5) indicate that there are seven main approaches to the study of social science. These include positivism, post-positivism, constructivism, the interpretive approach, the critical approach, feminism and post-modernism. However, the positivist, the post-positivist, the constructivist, the interpretive and the critical approaches receive more recognition according to De Vos *et al*. (2011:5). Corbetta (2003:12) on the other hand, is of the opinion that although there are various approaches to social science research, interpretivism and positivism are the two most important. He also argues that these approaches can be compared by analysing their philosophical origins by examining their views regarding ontology, epistemology and methodology (Corbetta, 2003:12). Marsh and Furlong (2002:20) chose interpretivism, positivism and realism as the most important approaches to social science research. Their categorising differs from Corbetta (2003:12) and De Vos *et al*. (2011:5) in that they are of the opinion that there is a distinct difference between positivism and realism, especially with respect to their ontological departure points. Although both are foundationalist in terms of their ontology, realists are of the opinion that there are relationships between social phenomena that are directly unobservable, but that are of great importance in behavioural explanation (De Vos *et al*., 2011:5).

With this detailed discussion as background, Figure 5 explains how these dimensions work together within the social science research process and how it relates to this study. These dimensions constitute the pillars of social science research. However, as depicted in Figure 5, the dimensions form layers. Every scientific research project with the main aim of understanding a particular phenomenon (central layer) is guided by an approach to ontology, epistemology and methodology (next layers). This process takes place within an

environment of collaboration and teamwork. Each approach within social science research adheres to a particular ontology, epistemology and methodology and therefore cuts across all the layers. These approaches or understandings determine how the researcher views the world, what the individual's place is within that world and how relationships are created within that world. For the purposes of this study, the aim is to understand the social phenomenon of social media by way of an anti-foundationalist ontology, interpretivist epistemology and a qualitative methodology, with a post-modern approach (see Chapter 3). Post-modernity best fits the focus of this study because it puts a premium on technology development and its impact on society. This study focuses on social media, which is a technology development that continuously changes and influences the environment.



Source: Own construct

Figure 5: Approaches to social research and the study of SOCMINT

With this discussion of research philosophy and dimensions of research as introduction and background, it is imperative to outline what the main components of social science research are.

2.4 Components of social research

The conceptualisation of social science research includes the research philosophy and the components of social research. The previous section discussed the philosophy and dimensions of social science research and explained how these form the framework for conducting social research. The discussion below examines the components for conducting social science research in detail.

The components of social research are based on a sound research philosophy and dimensions (Mouton & Marias, 1996:8), which consist of sociology, ontology, epistemology, teleology and methodology. Mouton (2007:179) refers to these components as "building blocks" of scientific knowledge that include research paradigms, definitions and empirical statements, conceptual frameworks and concepts. Although Mouton (2007:179) refers to four elements, this study goes further and views knowledge, discipline and tradition as part of the components or "building blocks" of research. The reason for this approach is that it provides a more detailed understanding and metatheoretical framework for this study. As explained earlier, intelligence studies is a young academic field with an underdeveloped theoretical base. This approach also contributes to building this theoretical base of intelligence studies.

For the purposes of this study, the discussion on the components of social science research should begin with the conceptualisation of knowledge and how it relates to science. This is important as it gives context and outlines the academic location of this study. According to the Concise Oxford English Dictionary (2004:1287), the word "knowledge" originates from 12th century Middle English, meaning "information, awareness and skills acquired through experience or education, the sum of what is known". Audi (2003:220) is of the opinion that "knowledge arises from experience, emerges from reflection and develops through inference". In relation to this study, "knowledge" is viewed as information gained through experience, observation and research. The term knowledge is indeterminate because it does not relate to one specific entity, but can have numerous connotations. Various authors (Mouton, 2011:138; Booth, 2007:1) have created models or elucidations to clarify the multiplicity of knowledge. These models indicate and highlight the different levels of knowledge. It is important to focus on this aspect, as not all knowledge is scientific and when dealing with academic research a certain type of knowledge is needed.

In his effort to explain and conceptualise knowledge, Mouton (2011:138) created a "Three-world framework". He explains that we live different lives every day, and in these different lives, we play different roles and need different kinds of knowledge (Mouton, 2011:138). World 1 is the world of "everyday life and lay knowledge", which is knowledge we gain from learning and experience (Mouton, 2011:138). This knowledge is also called "common sense, wisdom and experiential" and is of great importance when resolving problems in our everyday life. World 2 is the world of "science and scientific research" (Mouton, 2011:138). In this world, an unexplained phenomenon from World 1 is chosen for examination and it is researched to grow the body of knowledge. World 3 is the world of "meta-science" (Mouton, 2011:138). *Meta* is a word that has its origins in the Greek language, meaning "beyond" or "over". In science, it is of great importance to constantly re-look and reflect on research theory, methods and decisions to make sure that outcomes are valid, truthful and usable. Through this process, various meta-disciplines have been developed that assist in improving the science and scientific knowledge, expanding the knowledge base of a specific discipline.

Mouton (2011:138) explains in great detail the various types of knowledge that are encountered every day and the role they play. This is important, as not all knowledge is the same and not all knowledge can be treated as scientific. It is vital to explain what scientific knowledge entails and how it fits into the broader knowledge context to measure if a study is contributing to the scientific knowledge base.

While Mouton (2011:138) refers to knowledge in a "Three-world Framework", Booth (2007:1) categorises knowledge in the following manner:

- "Practical knowledge" – this is non-theoretical knowledge that you know and do on a day-to-day basis, such as how to drive a car or how to make coffee. This corresponds with Mouton's World 1.
- "Procedural knowledge" – this is knowledge related to rules and regulations within the community we operate in and which we have to abide by. These types of knowledge include rules such as not to overtake a car at a solid white line and to stop at a stop sign.
- "Operational knowledge" – this is knowledge developed through scientific research.

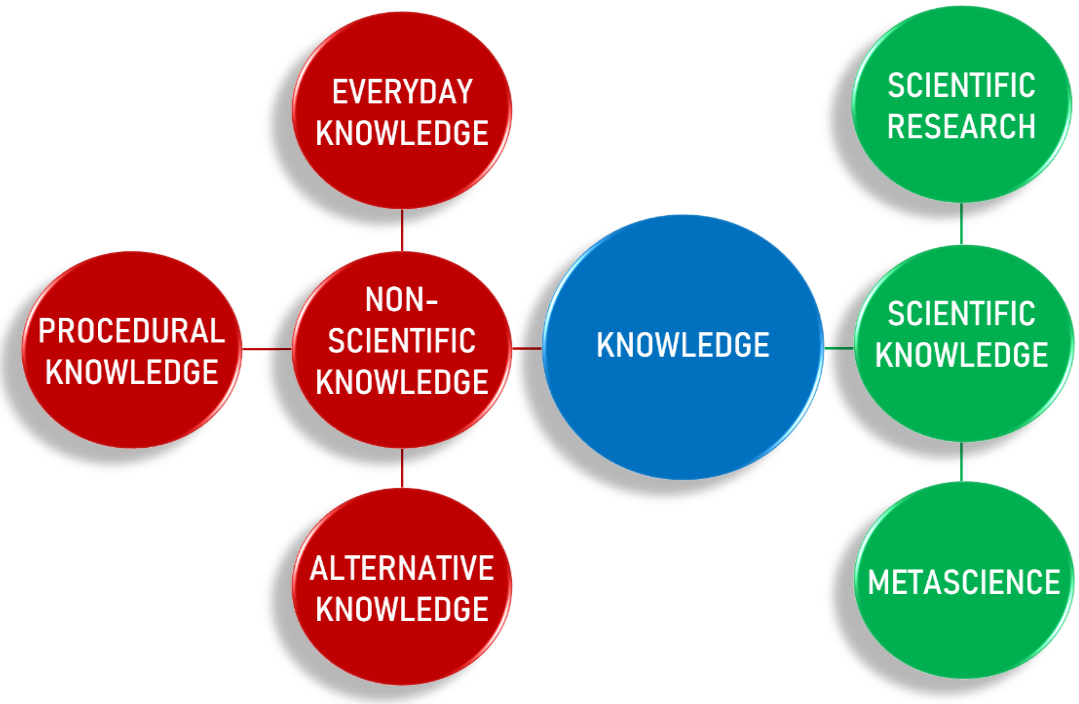
This framework discussed above is closely related to that of Mouton (2011:138); however, it includes "procedural knowledge", which could be included in Mouton's World 1. The most important knowledge relevant to this study is Mouton's World 2 and 3 and Booth's

operational knowledge. These types of knowledge are scientific and grow the body of knowledge.

In addition, De Vos *et al.* (2011:10) mention alternative knowledge, which is knowledge that is not based on research and is not necessarily correct. These alternatives include the following:

- Tradition: This is a "form of authority of the past" and is present in all societies. Everybody is born into a culture with its own knowledge and understanding of how things work or are supposed to work. This is passed down from generation to generation as the truth. This knowledge might have been true once, but with the passing down from generation to generation it does become inaccurate and unrelated to current situations.
- Authority: It is important to note that an authority in one area does not necessarily imply an authority on other matters. A professor in the field of economics is not necessarily an expert in politics, although he might have some insights into and opinions on that field.
- Personal experience: Personal experience can be a good source of knowledge, but it should not lead to over-generalisation.
- Common sense: This is a valuable source of knowledge as it is used on a daily basis, but it is not an alternative for scientific knowledge.
- Media myths: The media is an important source of information. However, it is not focused on accuracy, but rather on selling products or information. In the current environment. social media is an important source of information and knowledge. This has resulted in the latest concern of "fake news" (see Chapter 7), where everybody with a cell phone and access to the internet can be a journalist. This news is not always verified and is shared as the truth because it agrees with a certain narrative. "Fake news" increases the "media myths" type of information (De Vos *et al.*, 2011:10).

When analysing the above-mentioned models it is clear that there are various levels of knowledge. This knowledge is divided into non-scientific or non-academic knowledge and academic or scientific knowledge (Figure 6). The non-scientific knowledge includes everyday knowledge, procedural knowledge and alternative knowledge. Scientific knowledge on the other hand, relates to scientific research or operational knowledge and meta-science. The knowledge that is of concern to this study is scientific knowledge and this study attempts to grow this scientific body of knowledge with regard to intelligence studies.



Source: Own construct

Figure 6: Levels of knowledge

With this discussion as background and the components of social science research in mind, this study divides knowledge into two distinct areas: pre-scientific consciousness and scientific knowledge. The reason for this particular distinction is that researchers start off with a particular knowledge that guides them in terms of various decisions in relation to the topic and how to approach the research. The end result of the research is scientific knowledge. The next section focuses on pre-scientific consciousness or worldview as the first of the two knowledge areas mentioned above.

2.4.1 Pre-scientific consciousness or worldview

The starting point and the first component of research is the *pre-scientific consciousness,* also referred to as the *worldview*. The research process starts with an idea about something or a curiosity about something. Issues such as ideology, religious views and upbringing influence the researcher's idea. Vidal (2008:9) explains a worldview is a "coherent collection of concepts allowing us to construct a global image of the world, and in this way to understand as many elements of our experience as possible". In order to explain the concept of a worldview he presents six questions, each corresponding to a particular philosophical discipline (Vidal, 2008:4). These questions together with the religious worldview are depicted in Table 2.

Table 2: Worldview explained

QUESTION	PHILOSOPHICAL DISCIPLINE	RELIGIOUS WORLDVIEW (CHRISTIAN)
What is?	Ontology – model of reality	Matter and mind
Where does it all come from?	Explanation – model of the past	God
Where are we going?	Prediction – model of the future	Life after death
What is good and what is evil?	Axiology – theory of value	Concrete and fixed values
How should we act?	Praxeology – theory of action	Precise and concrete actions – as set out in the Bible
What is true and what is false?	Epistemology – theory of knowledge	Knowledge comes from the Bible and religious experiences

Source: Vidal, 2008:4

It is important to note that any research takes place with the researcher's worldview as a basis. Furthermore, a researcher's cultural background and ideological perspective play a key role in how the world is viewed. The approach to reality and how this reality should be interpreted and understood influences the field or topic of research, research philosophy and the methodology that the researcher adopts.

For the purposes of this study this approach to reality and how reality is viewed, is termed "pre-scientific consciousness", which corresponds to the ontological dimension mentioned previously. It is of great importance that the researcher highlights the pre-scientific consciousness that supports the study to give the reader an indication of the way in which the researcher views reality, knowledge and life in general. This study is based on the religious worldview, in particular the Christian worldview. The worldview is not only the starting point but it also forms the basis for any study. The research is done through these lenses and it indicates where views and arguments come from. If researchers are not aware of their worldviews, it will complicate their ability to argue positions. At the same time, it is important to highlight these views for the reader beforehand so that the reader can understand why the author makes certain assumptions or interprets problems in a certain manner.

As explained earlier, knowledge is divided into worldview and scientific knowledge. With the discussion of worldview as the first part, the subsequent section considers science and scientific knowledge.

2.4.2 Science and scientific knowledge

The second component of scientific research is science and scientific knowledge. Although the practice of science has been with us since Aristotle, scientists still disagree on the appropriate definition of science (Babbie, 2008:2). The concept of science has different meanings for different people. When asked for a definition of science, some people might describe individuals in a lab or mathematicians or even a subject at school. It is of great importance to outline what is implied by science and how this study contributes to science and scientific knowledge.

According to the Concise Oxford English Dictionary (2004:1287), science is "the intellectual and practical activity encompassing the systematic study of the structure and behaviour of the physical and natural world through observation and experiment". The term originates from the Latin *scientia* meaning knowledge and *scire* meaning know. In his definition Neuman (2006:7) refers to science as "social institution and a way to produce knowledge", which describes the body of knowledge and the process. Mouton (1996:13) on the other hand explains that science refers to both the "body of knowledge" that has formed over time or the "product" and the practice of scientists to acquire knowledge or the "process." The ultimate goal of science is to search for the "truth" or "truthful knowledge" (Mouton, 2011:138).

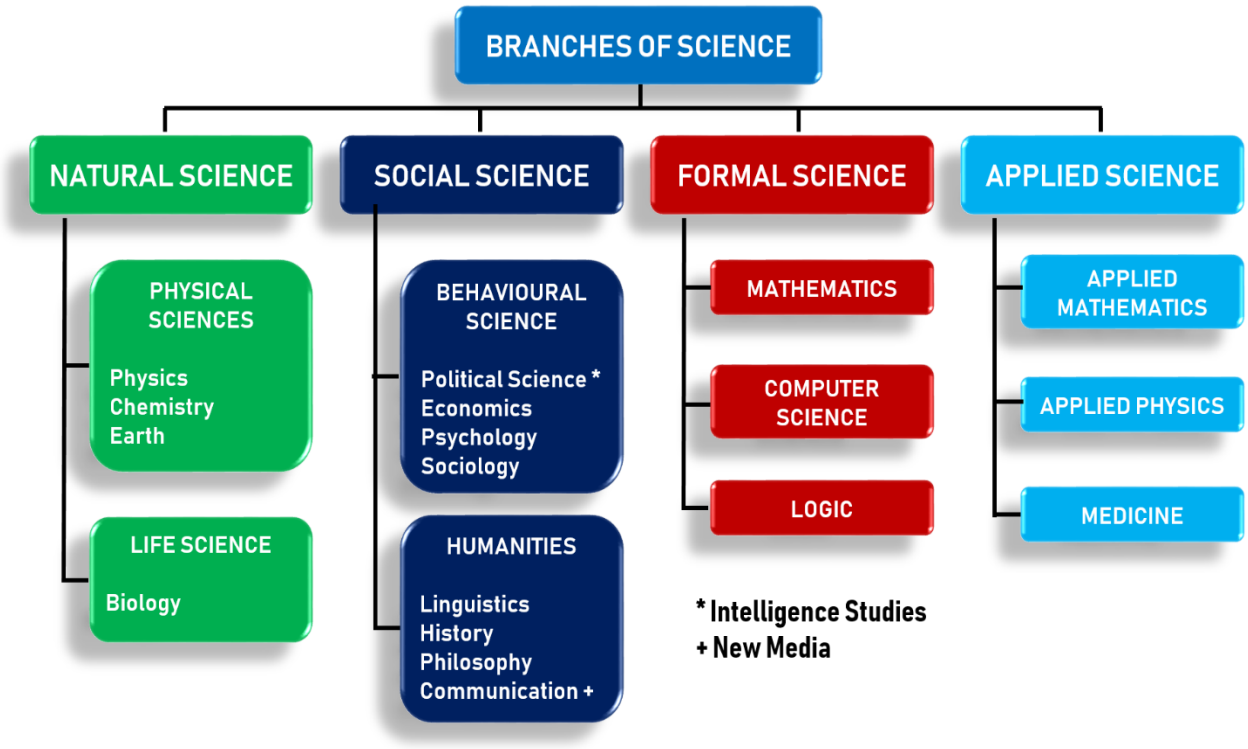
With these definitions and observations as background, it is clear that there is no single way to define science. It is also apparent that academics do not focus on the same aspects when describing science. Some highlight the method, others the action or the process, and others the result or outcome of the process. From these definitions, one can postulate the following definition: Science is acquiring and increasing truthful knowledge through observation, testing and experiments to understand the social world or a particular phenomenon.

In the case of this study, knowledge is increased through the observation of the social media phenomenon. This study attempts to understand the threats and opportunities social media holds for national security by observing the phenomenon. The residual value of social media is SOCMINT. This observation of social media aids the construction of a framework for SOCMINT.

With these explanations as an outline, what then are scientific knowledge and scientific research and why is it deemed to be of a better standard than alternative ways of obtaining or gaining knowledge? When referring to something as scientific it gives it a certain status. What are the characteristics of scientific knowledge? Bhattacherjee (2012:1) and Achinstein (2011:347–357) identify the following characteristics of scientific knowledge:

- Scientific research focuses on observable phenomena, which implies that researchers use their senses to collect the relevant information.
- The phenomena can be in the natural, physical or social area.
- Phenomena are explained through testable experiments.
- These experiments can be executed by other independent researchers to reach the same result.
- The results must be subjected to peer review and publication.
- Scientific research includes the measurement of actual or potential rate of error.
- Degree of acceptance within the scientific community.

The discussions thus far focused on science and scientific knowledge as a whole. However, it is necessary to break down science into its branches to position this study within a specific academic field. Although various classification systems are available, science can be divided into the following four broad themes or branches: natural, social, formal and applied sciences (depicted in Figure 7). Mouton (2007:9) divides the field of science into four areas, but he classifies social and humanities sciences as separate fields while they are usually classified together under behavioural sciences. According to Mouton (2007:9), science is classified as natural sciences (biology, physics and chemistry), formal sciences (mathematics, computer science and logic), social sciences (political studies, sociology, anthropology, economics) and humanities (history, linguistics, philosophy). While social sciences study human and cultural activities directly and usually in the present, humanities are more concerned with the indirect human activities. Whereas Mouton (2007:9) uses a comprehensive classification of sciences, Bhattacherjee (2012:1) only refers to two broad categories, inter alia natural science (naturally occurring phenomena) and social science (science of people or groups of people). Although this study subscribes to science as depicted in Figure 7, it only focuses on the natural and social sciences and broadly refers to the formal and applied sciences.



Source: Own construct

Figure 7: Branches of science

The main purpose of social research is to understand a certain phenomenon or phenomena related to society, their actions, relations and beliefs (Neuman, 2006:7). The French philosopher Auguste Comte (1798–1857) can be described as the father of social science as he created the term *sociology* in 1822. He recognised society as a phenomenon to be studied scientifically (Babbie, 2008:36). Before this time, the only known and acceptable field was natural science. Williams and May (2003:13) refer to social research as the "child" of scientific research because its origins only go back to the nineteenth century model of physical science. Since the inception of social sciences, there have been two diverse views on the theoretical framework of social science. The first view is that social sciences can share the same scientific framework of rules, generalisations and predictions that describe natural sciences (Henn *et al*., 2006:8–9; Williams & May, 2003:47). Others are of the opinion that the differences between social and natural sciences go far deeper than just the focus (Henn *et al*., 2006:8–9; Williams & May, 2003:47). They claim that social phenomena are sufficiently dissimilar from natural phenomena and therefore permit and are in need of a different scientific framework with its own methods, designs and systems. Social sciences study human beings who have the capacity to think and reason, which is not the case with the objects of study in the natural sciences. Therefore, social sciences need different scientific approaches from natural sciences.

At this point, it is necessary to compare these two sciences to highlight the different approaches and to assist in creating the metatheoretical framework for this study. Natural sciences, according to Ledoux (2002:34), are "disciplines that deal only with natural events using scientific methods". These sciences can be described as exact, detailed, unequivocal, and deterministic (Berg, 2001:15). Another important aspect of natural science is that it is autonomous from the researcher, implying that any person doing the experiment or observation will come to the same result or conclusion. In contrast, social structures or social phenomena do not exist separately or independently from the world or the researcher analysing the situation (Marsh & Furlong, 2002:24). Social phenomena and social structures are influenced by the environment surrounding them and they influence their surroundings. This suggests that the outcomes of experiments and observations might differ from researcher to researcher. This view is echoed by De Vos *et al.* (2011:5), who say that social sciences "deal with a particular phase or aspect of human society" and are sometimes called "soft sciences" because their subject matter is "fluid" and not measurable through instruments and experiments.

The table below highlights the differences between natural and social sciences.

Table 3: Comparison between natural and social science

NATURAL SCIENCE	SOCIAL SCIENCE
Deals with laws of nature and physical world	Deals with human behaviour
Hard science	Soft science
Relies more on experimental design	Relies on observation
Consensus on concepts and operational definition	Less consensus on which concepts are important
Molecules are predictable	Human behaviour less predictable
Autonomous from the researcher	Social phenomena are part of the world – cannot be autonomous
Old science	Young science
High predictability	Low predictability

Source: Own construct

Following this clarification of the branches of science, it is important to also clarify where this study fits in. This study is not the focus of one particular academic field or discipline. Although the main focus is on intelligence studies, it also straddles across the fields of new media studies and computer science. Therefore, in the main this study belongs to the

category of social sciences, which is the study of humans, human behaviour and the impact on the social environment. New media studies falls under the social sciences, while computer science belongs to the formal sciences. This study investigates the social media phenomenon (human behaviour) and how it affects national security (social environment).

This study is approached from the perspective of a Christian worldview and belongs to the social sciences. However, it is important to indicate to which discipline in the social sciences it belongs. In order to do this, the next important aspect or building block of social science research is discipline.

2.4.3 Discipline

It is necessary to specify the discipline that grounds this study. Each subject belongs to a certain discipline, which provides it with an important base and discipline-specific substance, such as theories, models and paradigms. The social science branch is divided into various disciplines, such as political science, economics, psychology and sociology. According to the Concise Oxford English Dictionary (2004:408), discipline is a "branch of knowledge, typically one studied in higher education". The term *discipline* has its origins in the Latin words *discipulus*, meaning pupil, and *disciplina*, meaning teaching. Before a subject can be classified as a discipline, it should display various characteristics. These characteristics include the following:

- A discipline has a specific focus of research (politics, economics, and sociology), which can overlap with another discipline.
- A discipline has a "body of accumulated specialist knowledge" specific to the research focus and not generally shared with other disciplines.
- A discipline has theories and concepts that help to organise the "accumulated knowledge" in a systematic fashion.
- Each discipline applies terminology and language specific to that discipline and focus area.
- A discipline uses research methodologies that have been established over time for their specific focus and needs in relation to that focus.
- A discipline's end result is institutionalisation, such as academic departments at universities or colleges (Krishnan, 2009:9).

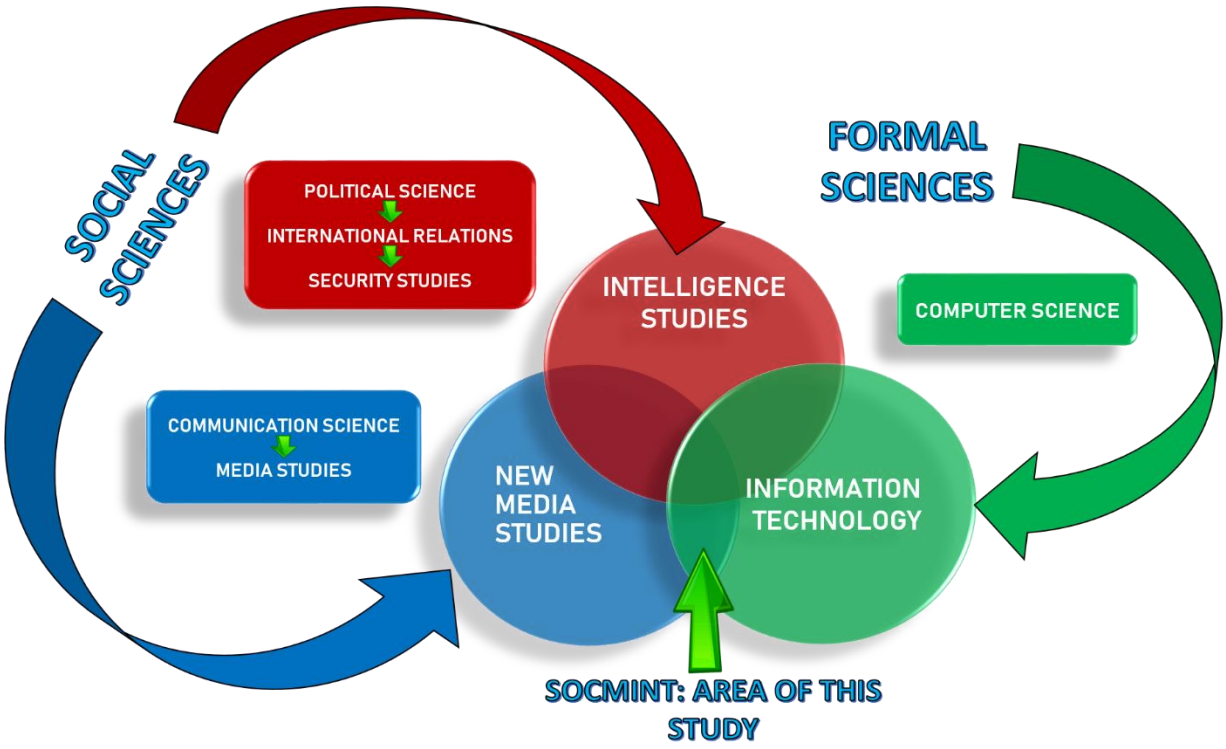
Together with the characteristics of a discipline, it is also important to indicate the functions of a discipline. The function of a discipline can be deduced from the above-mentioned characteristics. The functions are twofold: teaching and research, which leads to growth in the body of knowledge (Duvenhage, 1994:32).

For the purposes of this study, a discipline is an exact focused research area with accrued knowledge and with theories, tradition, language, terminology and methodology inherent to this area with the main focus of growing the body of knowledge. Intelligence studies belong to the discipline of political science (see Chapter 3). Although not a discipline yet, intelligence studies also has specific theories, traditions, language, terminology and methodologies, which are discussed in great detail in Chapter 3.

In this context, it is imperative to highlight the academic location of this study, which is in the main intelligence studies. Chapter 3 offers a detailed discussion of the academic roots of intelligence studies. It is important to note that this study has three pillars and has its roots in various disciplines and sub-disciplines within the branch of social sciences and the formal sciences. The first and the most important pillar is intelligence studies, which originates in the field of political science. Intelligence studies is discussed in much more detail as it is the centre of this study. The second pillar is media studies, which forms the basis for new media studies in general and social media in particular. The final pillar is information technology (IT), which provides the platform for the operation of new media and originates from the computer science discipline. IT is only highlighted in as much it is the enabler for social media and is not discussed in terms of its metatheoretical base. It is vital to highlight this consecution as it guides discussions in future chapters.

Intelligence studies is a young academic field that is directly linked to the sub-discipline of security studies under the sub-discipline of international relations. Together these sub-disciplines fall under the discipline of political science (Figure 8). The discipline of political science was only recognised as a separate discipline during the late eighteenth and early nineteenth centuries when political science departments were established at universities. However, the discipline was seen as inter-disciplinary for some time and was taught in history and economics departments. It was not until the twentieth century that political science was recognised as a discipline in its own right (Jackson & Jackson, 1997:21). One of the sub-disciplines under political science is international relations, which is a new discipline that only developed as a separate discipline after World War I (Hollis & Smith, 1990:16). Before World War I, international relations was mainly perceived as an inter-disciplinary field that formed part of political science, history, law and philosophy and not a

discipline on its own (Hollis & Smith, 1990:16). It was only after World War II that international relations was recognised as a sub-discipline of political science with the main aim of bringing peace (Cox, 2012:17; Frieden & Lake, 2005:1; Hollis & Smith, 1990:16). Security studies have its origins within international relations, specifically Western international relations linked to nuclear weaponry and the Cold War (Baldwin, 1995:117; Buzan & Hansen, 2009:1; Griffiths & O'Callaghan, 2002:289). Security studies is a relatively new discipline and according to Bock and Berkowitz (1966:122), the field of national security affairs is one of the most salient developments in post-World War II social science research.



Source: Own construct

Figure 8: SOCMINT: Convergence of various disciplines

The second pillar of this study is new media studies (illustrated in Figure 8), which is linked to media studies, which is a social science. Media studies belong to the discipline of communication sciences within the humanities. The third pillar of this study relates to IT, which is relatively new and a sub-discipline of computer science. In the broadest sense, IT refers to all kinds of technology that is used to create, store, exchange and use information in various forms (Concise Oxford English Dictionary, 2004:730). However, for the purposes of this study, the focus is on IT with the internet, computer and mobile phone network as foundations.

This study, with its main focus of SOCMINT, is a construction of three main disciplines. It is located within the sub-field of intelligence studies, which has its key origins in the discipline of political science. However, the social media aspect of SOCMINT also relates to the discipline of communication science and IT. The introductory paragraph of this section mentions the importance of grounding this study in a specific academic discipline. This study is founded on intelligence studies and political science and issues can be explained against this background. Political science underpins intelligence studies on issues such as traditions, theories, models and methodologies. Furthermore, issues can be explained from a political science perspective.

With this clarification of what a discipline entails and where this study fits in, it is important to discuss the components of a discipline. Each discipline has its own traditions, paradigms, conceptual frameworks and concepts that are relevant and unique to that specific field. The subsequent sections address these components in more detail.

2.4.4 Tradition

According to the Concise Oxford English Dictionary (2004:1528), *tradition* is defined as "the transmission of customs or beliefs from generation to generation". This is a more general view of tradition, but it can also be made applicable to the academic field and to the study of intelligence in particular. Within every academic field, there are beliefs, practices and principles that are handed down from research generation to generation. When starting with a study it is important that researchers familiarise themselves with that field to adhere to these values and fully understand the subject matter. Duvenhage (1994:37) has a more detailed view of tradition and he describes it as "a complex network of philosophy/ideology and mythological orientation linked to a specific discipline, which is historically grounded and influence research in that particular field". With reference to the intelligence field, Walsh (2011:29) defines traditions as "a set of beliefs, customs, practices, principles and accumulated experiences handed down from earlier generations of intelligence practitioners that inform contemporary practice". He furthermore articulates that intelligence traditions explain historical development and the uniqueness that distinguishes intelligence from other fields. It also helps us understand how it is applicable in new environments (Walsh, 2011:29).

While it is important to understand the traditions within the specific discipline, there is also a need to recognise the characteristics of a tradition. On this matter, Duvenhage (1994:33)

identifies the following characteristics (these characteristics are discussed in relation to political science, which is the discipline where intelligence studies originate):

- A tradition emphasises the distinctive characteristics, research focus, philosophy and history of a particular discipline (Duvenhage, 1994:33). The subject tradition differentiates political science from psychology or economics. Even though intelligence studies is not viewed as a discipline, this characteristic is also true for the field of intelligence studies, which has its own focus area of research, philosophy and history.
- Tradition is grounded in the scientific or research history of the particular discipline or field of study (Duvenhage, 1994:33). In relation to the development of political science, Easton (1991:275–290) identifies four stages: formal (study focused on an understanding of the laws governing power, which leads to an understanding of operations of political institutions), traditionalism (study of political parties and growth of pressure groups), behaviouralism (focus on the behaviour of the human actor) and post-behaviouralism (study of new social issues such as environmental pollution, nuclear war and social equality). As mentioned previously, intelligence studies is a relatively new academic field that does not yet have a rich history as is the case with political science. However, the field of intelligence studies has since its beginning in the late ’50s favoured the realist tradition (see Chapter 3).
- A tradition constitutes various smaller sub-traditions in relation to philosophy and methodology (Duvenhage, 1994:33). In reference to philosophy, some of the major approaches within the field of political science are liberalism, conservatism and socialism (Jackson & Jackson, 2003:162–167). Equally important is the methodological sub-traditions within political science research. Some of these include the traditional-historical approach, the behaviouralist and post-behaviouralist approaches, and the systems approach (Jackson & Jackson, 2003:27–31). Robertson (cited in Classen, 2005:31) identifies four main approaches to the study of intelligence in the United States of America. The first of these approaches is a series of early works in the post-war period with Sherman Kent as one of the key role players. The second approach is the liberal school, which is based on the foundation that intelligence activities create problems for democratic values. The main supporter of this school was Harry Howe Ransom. The surprise school is the third approach, which is also called the historic school, with Roberta Wohlstetter as one of the main sponsors for this approach. This approach focuses on examining intelligence failures and successes to deduce lessons from these events. The fourth and final approach is the realist school that argues that intelligence is necessary and desirable. A major proponent of this school is Ray Cline.

It is important to highlight some traditions from the intelligence field. Intelligence studies is a relatively new academic field, which is also reflected in the lack of broad international academic contributions. The USA remains one of the most influential role players with regard to intelligence studies (Lowenthal, 2006:11). Therefore, the USA is used here to illustrate tradition within the field of intelligence studies. According to Walsh (2011:29), there are three characteristics that describe intelligence tradition: the security environment, secrecy and surveillance. The intelligence community has to provide information to the decision maker with regard to the security environment, which includes threats against and opportunities for national security. This comprises the national and the international area of influence of the country. In order to provide the decision maker with forewarning, information is obtained through the use of sources or through technical means. Secrecy is therefore of great importance to protect sources and the information. One of the most important ways to provide forewarning is through surveillance. The current global environment has necessitated an increase in surveillance through technical means (SIGINT). This study with its focus on social media and the use of the information obtained through social media (SOCMINT), also falls in the surveillance category and is in support of the intelligence traditions. Walsh (2011:29) recognises that although there are other characteristics that can also be included, these three have been central in explaining what intelligence is. For the purposes of this study, the intelligence cycle (the intelligence cycle is discussed in great detail in Chapter 3) is also added as a tradition. The intelligence cycle has always been part of the profession and is still used to explain how the different components of intelligence (collection, analysis, production and dissemination) are incorporated into the intelligence process.

As the second pillar of this study (see Section 2.4.3), it is also important to highlight some aspects in relation to traditions within new media studies. Craig (1999:135–149) distinguishes seven traditions within communication studies, each of which focuses on a different aspect of the field. These traditions include rhetoric, semiotics, phenomenology, cybernetics, social psychology, sociocultural theory and critical theory (Craig, 1999:135–149). These traditions are discussed in more detail in Chapter 4.

Tradition plays a key role in the academic research process. It guides the researcher with regard to the historical perspectives within the particular field and its application within the global environment. For the purposes of this study, a tradition is defined as a collection of philosophical and methodological insights. It is passed on through history and it influences studies in the field of intelligence. This study views the security environment, secrecy,

surveillance and the intelligence cycle as intelligence traditions. It is these traditions that give intelligence studies its uniqueness and influences research within the field.

Just as there are various traditions that are unique to specific disciplines, there are paradigms that are equally unique to certain academic fields. There are various paradigms within each discipline and it is therefore important to discuss paradigms as the fifth component of social science research. The next section elaborates on the issue of paradigms.

2.4.5 Paradigm

There is more than one way of looking at the same phenomenon and underlying each approach is a *paradigm*. The Concise Oxford English Dictionary (2004:1037) defines a paradigm as "1) a typical example, pattern or model of something, and 2) a worldview underlying the theories and methodology scientific subject". Neuman (2006:41) provides a more detailed definition and describes it as an "integrated set of assumptions, beliefs, models of doing research and techniques for gathering and analysing data". Babbie (2008:34), however, concisely defines a paradigm as "a model or framework for observation and understanding, which shapes both what we see and how we understand it". In addition, Babbie (2008:12) is of the opinion that it is impossible for people to be objective about the "real" world. Our views on social issues result from the paradigms into which we were born. This study subscribes to the notion that the way we think and argue about social issues is determined by the paradigm with which we grew up. For the purposes of this study, a paradigm is regarded as a world view or set of assumptions, which grounds the methodology and theory of the specific research.

One cannot fully understand paradigms within the social sciences without studying the views of one of the most influential intellectuals in the area of social science research, Thomas S. Kuhn. His book, *The structure of scientific revolution* (first published in 1962), has received a great deal of attention, especially in relation to paradigms. Kuhn (1996:12) argues that there are two interchanging phases in the history of any science, a period of "normal science"[13] and a period of "revolution". Scientists work and perform research within the framework of the given or recognised paradigm of that period, which Kuhn (1996:12) calls the "normal science". As research is done, inconsistencies appear and as more inconsistencies appear,

[13] According to Kuhn (1996:10), "normal science means research firmly based on past scientific achievements, achievements that some particular scientific community acknowledges for a time as supplying the foundation for its further practice".

the legitimacy of the recognised paradigm becomes questionable and the continuation of this paradigm becomes unsustainable. This eventually leads to a new paradigm and Kuhn (1996:12) views this as the “revolution” in scientific thinking. This new paradigm then becomes the “normal” and research continues within the structure of this paradigm.

In analysing the structure of a paradigm, it is clear that it comprises various components, each playing a specific role. According to Mouton and Marais (1996:146–147), the various components of a paradigm include theory, methodology, metaphysics and the scientist or researcher. The study of specific paradigms reveals that researchers make various commitments to these components of a specific paradigm. These include commitments in relation to a specific theory (forms the core of the paradigm), methodology or research techniques (as dictated by the paradigm), metaphysical assumptions (research object) and assumptions the scientists make themselves (Mouton & Marais, 1996:146–147). Furthermore, when a paradigm is adopted by a group of researchers or a discipline, this implies that the specific paradigm is the best option. These commitments then provide a point of departure for the researcher and guide the research process. In addition, the paradigm fulfils a certain role and function in the research process. The functions of a paradigm are to identify the problem, to collect relevant data, to problem-solve by synchronising data and theory, to predict results, and the articulation and expansion of existing theories (Mouton & Marais, 1996:147–149; Duvenhage, 1994:40). These functions are very important in academic research to assist in growing the body of knowledge.

When we turn to paradigms within the intelligence field, it is important to take the current global environment into consideration. The increased pace of globalisation has brought with it serious challenges to international security as it has created a borderless environment where transnational criminal activities could take place. This transnational phenomenon necessitates a new intelligence paradigm (Lahneman, 2010:201). The main objective of intelligence is to obtain, collate and disseminate information to the government of the day timeously to assist with decision and policy-making. However, since the end of the Cold War, intelligence communities have been in crisis because they did not predict the end of the Cold War and were not ready to deal with new challenges. Lahneman (2010:203) is of the opinion that intelligence communities are still operating on the basis of the Cold War paradigm where threats were small in number, mainly military, and sources of information were limited. During the Cold War, military experience gained during World War II and the perceived threat of Communism formed the bases for the intelligence paradigm, and security policies were aimed at the state (Coyne *et al*., 2014:54). This narrow approach to intelligence proved problematic after the end of the Cold War, which exposed a great number of threats related

to transnational activities, such as drug trafficking, human smuggling and terrorism. Although these threats did exist and were on the priority lists of major intelligence agencies, they were not viewed as major threats to the state (Walsh, 2011:14).

With globalisation and the major changes in communication technology, the Cold War paradigm no longer serves the intelligence community optimally. The intelligence environment has changed and the intelligence community should take cognisance of the following:

- Vast open source information is now available and the intelligence environment should have the ability to extract critical information.
- It is crucial to understand global dynamics and human activities. Information sharing among agencies and even countries has become essential to create a complete picture.
- Analysts have to focus more on the prevention of a potential threat than reacting to a threat that has already transpired (Coyne *et al*., 2014:57–58; Lahneman, 2010:203).

With this in mind, Lahneman (2010:209) proposes a paradigm of "adaptive interpretation" that involves "complicated puzzles for which virtually all the pieces are available". These pieces are across the world and therefore information sharing and updating of the information is crucial to complete the picture.

In order to create a complete picture of the metatheoretical framework of this study, it is important to also highlight paradigms in media studies, especially theory in relation to new media, as social media is classified as new media. New media is any form of media that is not in old media format, in other words media that existed before the internet. Newspapers, magazines, television, film and radio are examples of old media. Scolari (2009:946) is of the opinion that the term "new media" is not appropriate because all "new media" is "old" at some stage. He argues that terms such as "hypermedia", "networked", "collaborative communication" or "digital communication" should rather be used. The traditional communication methods are currently being confronted by the new generation of digital media (Scolari, 2009:944). It is therefore imperative to discuss a paradigm relevant to new digital media. A detailed discussion of the digital media paradigm appears in Chapter 4.

A paradigm may change when challenged with new research outcomes. It is the opinion of the author that a new intelligence paradigm is necessary. The old Cold War paradigm based on the military threat of Communism is no longer relevant and a new intelligence paradigm is

needed to accommodate new emerging threats. Such a new intelligence paradigm should not just focus on the analysis part ("interpretation"), but should include intelligence in its totality (collection, analysis and dissemination). Such a paradigm is called the "interactive and interconnected" paradigm for the purposes of this study. This implies that the intelligence community collaborates (interactive) with other security communities while also being connected to the new global environment. The new communication technology has created a wholly different threat environment than the threats the intelligence community was used to during the Cold War era. The new threat operating within the realm of the internet and its communication systems is faceless and is not restrained by borders. Furthermore, the new ICT has created a situation where information is abundantly available, accessible and produced at an alarming rate, making it increasingly difficult for the intelligence community to extract the relevant information. The challenge is to collect and identify the most crucial and significant facts, interpret it and provide it timeously to the decision maker in order for the intelligence services to remain relevant.

Against this backdrop, the next section focuses on the conceptual frameworks that are of importance within the social science research process.

2.4.6 Conceptual frameworks

The sixth component of social science research is *conceptual frameworks*. There is no fixed way to define conceptual frameworks and in the most cases, the term is used without proper definition (De Vos *et al*., 2011:35; Jabareen, 2009:51). However, it is of great importance to understand this concept as it forms an integral part of social science research. Some authors describe it simplistically as the key issues that will be studied, the connections between them (Miles & Huberman, 1994:18) and an "argument about why the topic one wishes to study matters" (Ravitch & Riggan, 2012:5). However, a more comprehensive explanation is needed to clarify this concept. It would be more correct to define conceptual frameworks as the integration of scientific statements into a certain framework, and in doing so, creating the structures of science (typology, models and theories) (Jabareen, 2009:51; Mouton & Marais, 1996:136). It is also imperative to note the features or characteristics of a conceptual framework. These features include the following:

- Each concept plays an important role in the study and all the concepts must be seen as a collective.
- A conceptual framework provides an interpretive approach to social phenomenon.

- Conceptual framework within qualitative research offers an understanding of the social phenomenon.
- A conceptual framework can be constructed through qualitative analysis (Jabareen, 2009:51).

For the purposes of this study, a conceptual framework is understood to be the combination of concepts, constructed through qualitative analysis, which explains and provides an understanding of a social phenomenon. The conceptual framework of this study explains intelligence studies and new media studies. With the definition clarified, there is also a need to discuss the various conceptual frameworks. Mouton and Marais (1996:135) identify three conceptual frameworks: typology ("classifying or categorising single variables"), models ("provides a systematic representation of phenomena by identifying patterns and regularities among variables") and theories ("provides an explanation of phenomena by postulating an underlying causal mechanism"). This study considers how these conceptual frameworks apply to the different disciplines linked to this study.

According to Mouton and Marais (1996:135), typology is the most basic conceptual framework, also referred to as "classification". The Concise Oxford English Dictionary (2004:1560) describes typology as a "classification according to general type, especially in social sciences". This classification is done according to common characteristics such as race, gender or language. Mouton (2007:196) recognises three characteristics of typology:

- "Type is the basic unit" where the most important characteristics of the phenomenon are highlighted.
- "No type is ever an exact replica of all the characteristics of a phenomenon" where the link between the type and the phenomenon is an estimate.
- "The criteria of good classification and in the case of typology is exhaustiveness (include all possible characteristics) and mutual exclusiveness (no overlap between categories)".

With regard to typology in intelligence studies, the most commonly used is that of intelligence services. There are different types of intelligence services, and the type depends on the type of state or government. With regard to new media studies, the typology that would be of importance to this study is the distinction between old and new media. The old media refers to broadcasting, cinema and print media while new media includes digital, interactive and computer-mediated communication. Typology is addressed in Chapter 3 (intelligence studies) and Chapter 4 (new media studies).

The second conceptual framework is a model, which is defined as “a simplified description, especially a mathematical one, of a system or process, to assist calculations and predictions” (Concise Oxford English Dictionary, 2004:918). According to Blaikie (2010:21), models can refer to, “a hypothesised set of relationships between concepts, explaining mechanisms or a method to organise research results”. Theories and models are sometimes used interchangeably (Blaikie, 2010:21; Mouton & Marais, 1996:138; Van De Ven, 2007:143). However, models are “partial representations or maps of theories” and because theories are not “directly observable”, they have to be operationalised into a “research model” (Van De Ven, 2007:143). It would be applicable to argue that models depict theories for a better understanding of the latter.

Just like with typologies, models also have certain characteristics unique to this conceptual framework. Gorrell (cited by Mouton & Marais, 1996:141) identifies the following characteristics:

- A model ascertains the crucial problem in relation to the phenomenon that should be examined.
- The model simplifies the problem that is being investigated.
- In some instances, the model offers new language or definitions for discussion of the phenomenon.
- Models also serve as tools for explanations and predictions.

The above-mentioned characteristics underline the idea that models help us understand theories. Within the intelligence field, the model that is most often used and cited is the intelligence cycle (Figure 9). The intelligence cycle describes the process of intelligence and is the first step in understanding intelligence. Although the cycle is used as a model to describe the intelligence process, various authors are of the opinion that the cycle does not appropriately describe the intelligence process (see Chapter 3).

Source: Adapted from Walsh, 2011:92

Figure 9: Intelligence framework

The third conceptual framework is theories. The Concise Oxford English Dictionary (2004:1495) defines theory as "a supposition or a system of ideas intended to explain something, especially one based on general principles independent of the thing to be explained". According to Neuman (2006:24), theory has a prominent role in research. He defines a theory as "a system of interconnected abstractions or ideas that condenses and organises knowledge about the social world". In addition, theories within the social sciences explain and predict social phenomenon in a systematic manner (Babbie, 2008:13; Heywood, 2002:20; Risjord, 2014:38; Sayer, 1992:50; Viotti & Kauppi, 1999:3). It is important for a researcher to be clear and articulate when presenting the theory as it assists the reader to read and understand the research (Neuman, 2006:25).

A "good" theory has the following characteristics:

- It consists of various concepts.
- Each concept implies assumptions that are part of that concept. The concept of a car has built into it the assumption that it can move and that it needs fuel of some kind.

- A theory explains the relationships between the concepts that form part of that theory. It explains why there is or is not a relationship and how that relationship is structured. These concepts and the relationships are explained in a logical and consistent manner.
- In order for a theory to be valid, it must be testable and falsifiable (Bhattacherjee, 2012:28; Neuman, 2006:26–29; Popper, 2002:96).

From the discussion, it is clear that theory, particularly within the social sciences, explains a social phenomenon and may assist in predicting the outcome of similar events. Some of the most important theories within intelligence studies include realism and post-modernism (see Chapter 3). In relation to media studies, theories that play an important role in specifically social media is social network theory, gratification theory and interactivity theory, which are discussed in Chapter 4.

With the explanation of typology, models and theories as background, the next section elaborates on definitions and concepts, which is the final component of social science research.

2.4.7 Definitions and concepts

The most basic, but also important component of scientific research is concepts and definitions. It is essential to define concepts for the reader to understand the meaning and the researcher's interpretation of that specific concept. The Concise Oxford English Dictionary (2004:376) defines a definition as a "formal statement of the exact meaning of a word". According to Mouton (2007:187), a definition is "a statement that delimits or demarcates the meaning in terms of its sense and reference". Thus, a definition is a statement explaining the meaning of a word or phrase to have a clear and collective understanding. Mouton (2007:188) differentiates between two types of definitions, theoretical and operational definitions.

For the purposes of this study, theoretical definition is explained as the common purpose or meaning of the word or concept (Mouton, 2007:188). Words have different meanings or connotations that depend on the acceptable theoretical framework of that time or period. An operational definition is used to clarify the meaning of a specific word or concept. It converts the meaning as given by the theoretical definition into a measurement with specific conditions only binding during the use of that concept (Mouton, 2007:188).

The last and final component of social science research is concepts. The Concise Oxford English Dictionary (2004:296) describes a concept as “an idea or mental picture of a group or class of objects, formed by combining all their aspects”. This component is the “building blocks of theories” (Blaikie, 2010:111; Neuman, 2006:26) and “the most elementary symbolic construction by means of which people classify reality” (Mouton, 2007:180). Even though it is described as the most elementary, it is one of the most important components of research. It is imperative that the researcher clarifies concepts used in the study and clearly indicates the meaning assigned to that particular concept to make sure that the reader understands the researcher’s point of view.

Deleuze and Guattari (1994:15–21) offer a philosophical description of concepts from which the following characteristics can be construed:

- A concept is never “simple” as it involves various “components” that “define” it.
- Every concept has a history.
- Concepts relay back to other concepts.
- A concept is not created from nothing.
- Every concept must be understood within the context in which it is being applied.

Another important contribution in relation to clarifying concepts is that of De Vaus (2001:24). He is of the opinion that concepts are not “directly observable” (De Vaus, 2001:24). We cannot see concepts such as intelligence. For us to be able to “translate concepts into something observable”, the concept should be “operationalised” (De Vaus, 2001:24). This implies that we have to convert the concept into a measurable unit. This is in agreement with Mouton’s (2007:188) operational definition. For example, in the case of intelligence, the measurable unit is the intelligence quotient. Another helpful clarification of a concept is Neuman’s (2006:26) view that a concept consists of two pillars: a symbol (word or term) and a definition. The definition is crucial as it ensures that the concept is understood and interpreted in the same way.

With these explanations in mind, concepts can be defined as a researcher’s explanation or interpretation in relation to a specific phenomenon. This is of great importance because the reader has to understand the researcher’s views of the specific phenomenon to be able to comprehend the phenomenon and the outcome of the research process. Concepts ensure that everybody has the same departure point. Within the field of intelligence, the definition of intelligence is highly debated, as will be illustrated in Chapter 3. Concepts that are explained

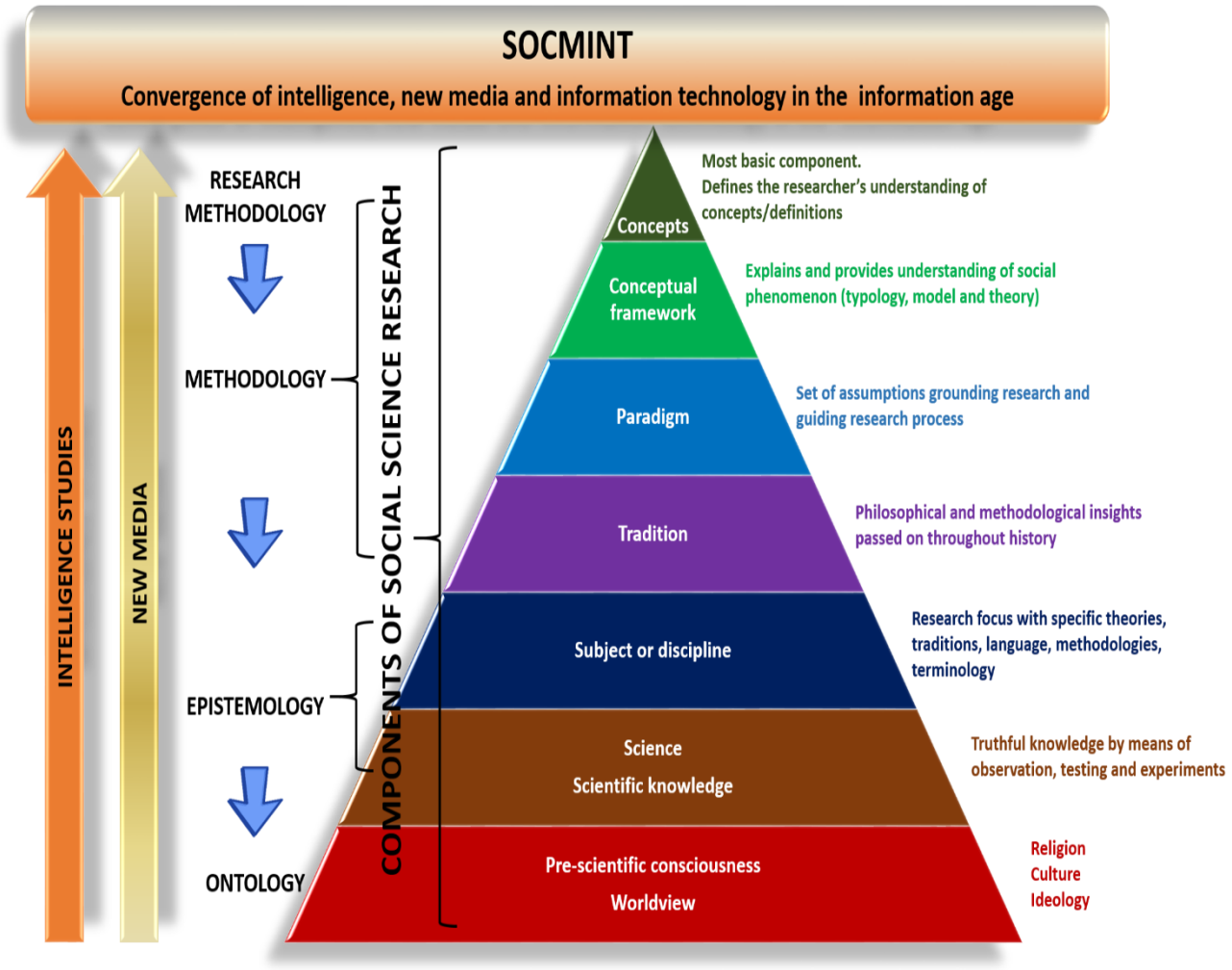
in the next chapter include intelligence and security. With regard to media studies, some concepts that should be clarified include new media, social media, social networks and social media platforms (Chapter 4 and Chapter 7).

This section focused on the seven components of social science research. Each component was discussed in detail and applied to intelligence studies and new media studies. The subsequent section combines all the previous discussions into one conceptual framework to understand social science research.

2.5 Metatheory to understand SOCMINT

The above discussion relates to social science research in general. These general components now have to be put into a framework that could be applied to this study to develop the metatheoretical framework for SOCMINT. This application is illustrated in Figure 10.

In the sketch, social science research is divided into two areas: components of social science research on the one hand and research philosophy on the other hand. These areas are interrelated. The research philosophy comprises ontology, epistemology and methodology, while the social science research components include pre-scientific consciousness or worldview, science and scientific knowledge, subject or discipline, tradition, paradigm, conceptual framework and concepts. Both the philosophy of research and the components of social science research are applied to the two pillars of this study, intelligence studies and new media studies. The convergence of the two pillars of intelligence studies and new media studies allows the construction of SOCMINT, which would in turn grow the knowledge base within intelligence studies.



Source: Adapted from Duvenhage, 1994:60; Greffrath, 2015:29

Figure 10: Conceptual framework for understanding social science research in reference to SOCMINT

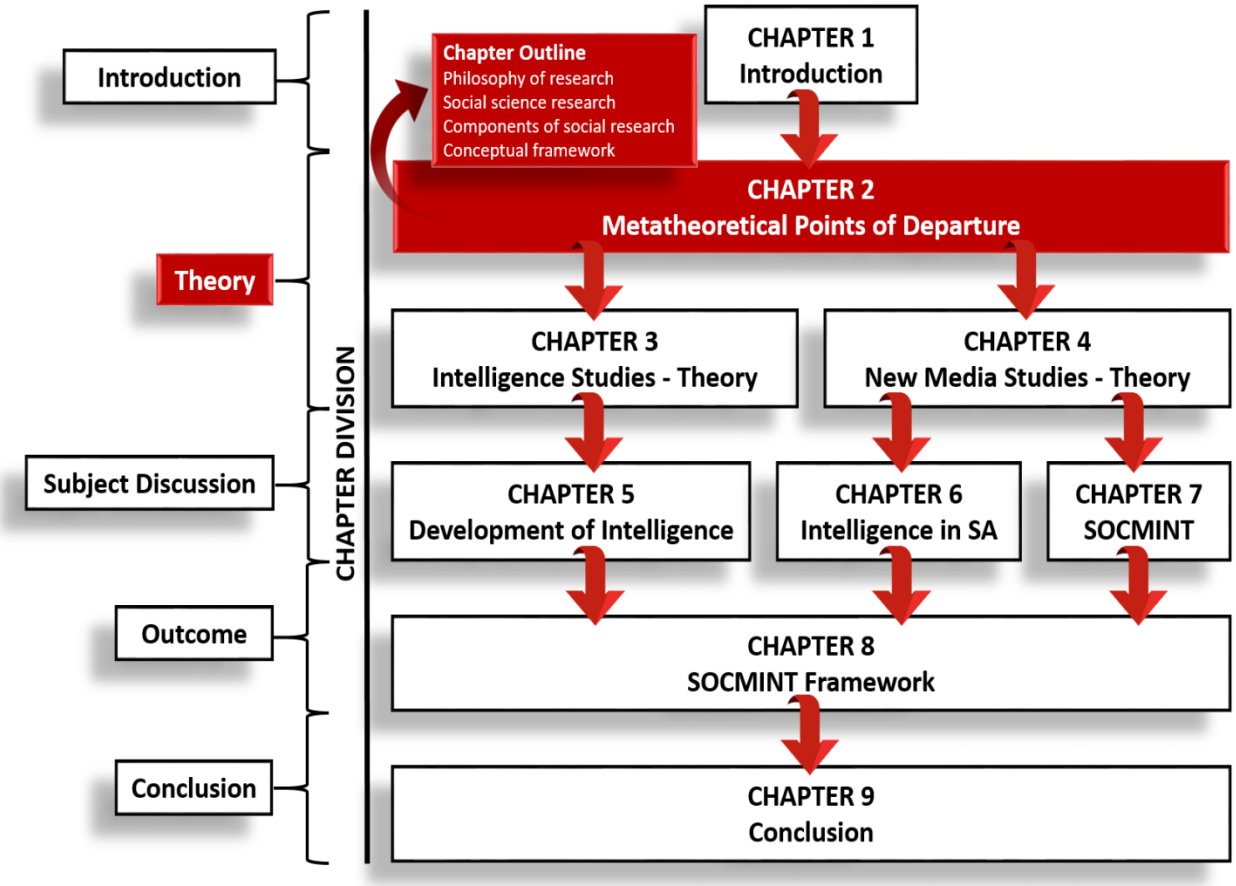
The ontology, which is the science of being, relates to the first component of social science research, namely pre-scientific consciousness. The component of pre-scientific consciousness forms the basis for social science research as it influences the researcher in terms of the topic, the research method and arguments. Epistemology is the science of knowledge and relates to scientific knowledge and discipline in the model above. It is important that the study complies with the characteristics of scientific knowledge to contribute to growing the body of knowledge. The research topic resorts under a certain academic discipline and should therefore adhere to the principles of that discipline. The next important pillar of research philosophy is methodology. This is the "how" of research and is relevant to tradition, paradigm, conceptual framework and concepts within social science research. These components determine the way in which research is conducted and what the theoretical grounding is in terms of the paradigm, conceptual framework and concepts.

The outcome or end goal of this metatheoretical framework is the growth in the body of knowledge.

2.6 Conclusion

This study is an attempt to take the challenges of the information age head on and to create a new approach to intelligence. The main purpose of this chapter was to reflect on the metatheoretical framework for this study and to illustrate how this study will grow the body of knowledge in relation to intelligence studies. Intelligence studies is a relatively new academic field and to grow into a discipline, the theoretical base should be expanded. Metatheory is the philosophy behind a specific theory and provides a framework to guide research. One way in which the theoretical base can be broadened and deepened is to focus on and understand the metatheory behind the theory.

Figure 11 summarises the outcomes of this chapter and positions it within the framework of this study.



Source: Own construct

Figure 11: Chapter 2 Summary

The objective of this chapter was to construct a metatheoretical framework to guide this study. The metatheoretical framework supports the main aim of this study, which is the systematic investigation of intelligence studies and social media to construct a strategic framework to incorporate the new phenomenon of SOCMINT into the intelligence environment. In an effort to reach the objective of a metatheoretical framework, the following goals were addressed:

- to identify, define and discuss the major social science components;
- to apply these components in the context of intelligence studies and media studies, new media in particular; and
- to construct a metatheoretical framework to guide this study and the understanding of SOCMINT.

The social science research components were identified as pre-scientific consciousness, science and scientific knowledge, subject or discipline, paradigm, conceptual frameworks and concepts. These components were conceptualised within the context of social sciences and applied to intelligence studies and new media. All the components have been explained in relation to social science research. However, with regard to intelligence studies and new media studies, only the relevance and application of ontology and epistemology were discussed in great detail. The third component, methodology, was highlighted and is discussed in more detail in the next chapter in relation to intelligence studies and in Chapter 4 with regard to new media studies.

To summarise the main outcomes of this chapter, this study subscribes to anti-foundationalist ontology, an interpretivist approach in relation to the epistemology and a qualitative research methodology. Furthermore, this study supports a Christian worldview and belongs to the social science branch and the discipline of political science. With respect to the paradigm, the current global situation of a borderless environment created by new communication technology has necessitated a new paradigm. The old Cold War paradigm is no longer relevant. This study subscribes to an interactive and interconnected paradigm, where the intelligence community is aware of and collects relevant information (interactive) and actively shares information with other intelligence services or law enforcement agencies (interconnected). Sharing is of utmost importance in this new borderless environment.

The chapter concluded with a conceptual framework for understanding SOCMINT. This framework illustrates how this study fits into the social science framework and that it is a convergence of two main disciplines.

The metatheoretical framework forms the basis for the following chapters and guides the research process. The next chapter focuses on the conceptualisation of intelligence by highlighting its academic origin, theoretical approaches and central concepts.

CHAPTER 3: INTELLIGENCE STUDIES: METATHEORETICAL, THEORETICAL AND CONCEPTUAL ORIENTATION

While the literature on intelligence actually goes back several millennia, it has only recently become sufficiently popular with scholars to warrant scholastic acceptability.
Stafford T. Thomas (1988)

3.1 Introduction

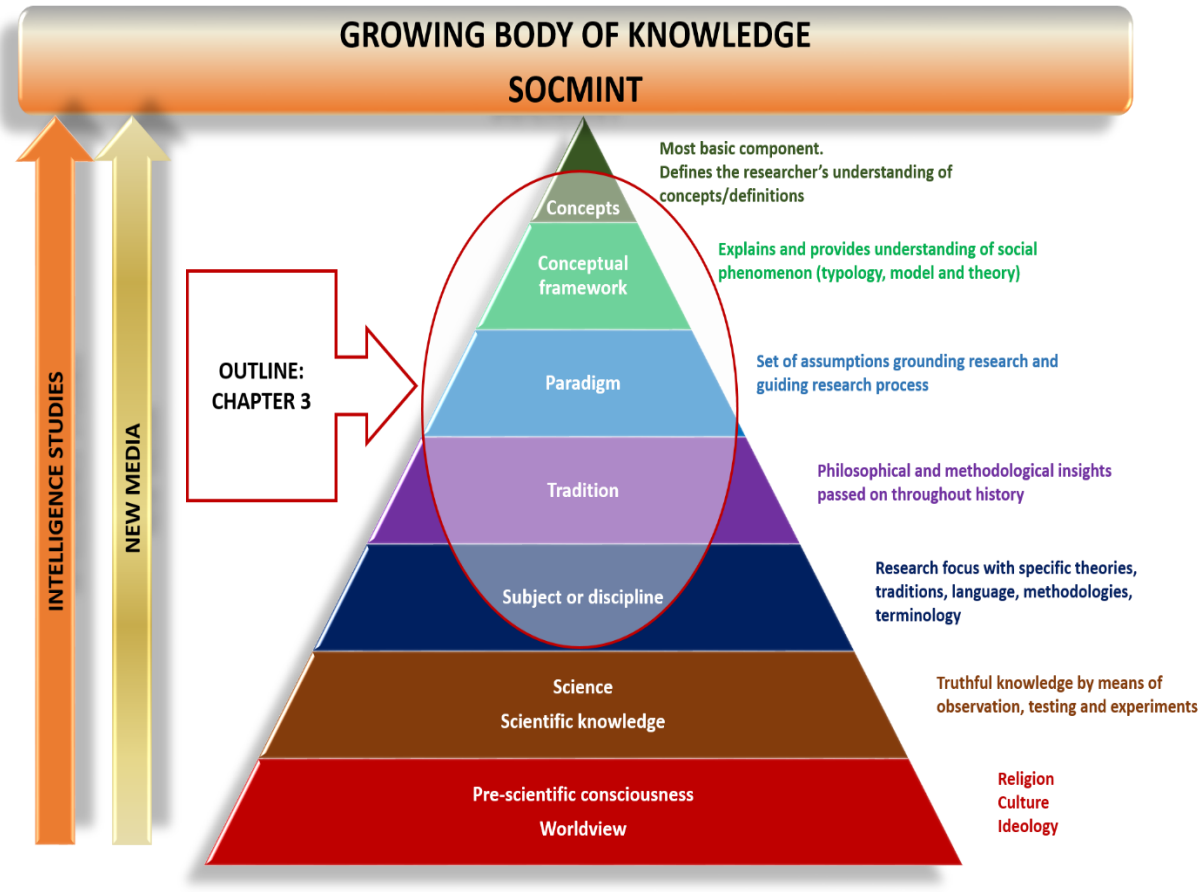
Chapter 2 provided a detailed metatheoretical framework for the conceptualisation and understanding of social science research, with specific reference to SOCMINT. In broad terms, the metatheoretical framework explains that this study combines intelligence studies and new media studies. However, intelligence studies forms the foundation and should therefore be discussed in detail.

Even though intelligence has been part of civilisation from early on, the field of intelligence studies in general and the theoretical basis in particular, remains in its early stages. Literature relating to intelligence studies has increased over the past ten to fifteen years, especially in terms of theoretical writings[14]. The increased availability of literature is mainly due to two reasons. The first is the process of declassification, which started just after the end of the Cold War. This opened the intelligence field to academics and provided them with the opportunity to analyse and comment on issues that were in the secret domain before. The second reason for the increase in literature is the 9/11 attacks. This event amplified the importance of intelligence in the public domain and subsequently encouraged a proliferation of literature. This being said, the theoretical base of intelligence studies remains weak. Gill *et al.* (2009:2) are of the opinion that the theoretical aspect of the field remains underdeveloped. Bay (2007:i) refers to it as "very much at an adolescent stage". There is an urgent need to increase and deepen the theoretical base of intelligence studies so that it could grow as an academic field. This study is an attempt to grow the knowledge and theoretical foundation to ultimately assist with the development of intelligence studies.

Against this background, the main focus of this chapter is to conceptualise intelligence. In order to reach this goal, the methodology is to apply the social science framework that was

[14] Intelligence literature receives contributions from three areas: academics who are not in the field of intelligence and who write purely from an academic perspective; practitioners-turned-academics who write from experience; and finally the journalist. All of these contributors write from their own perspectives based on the information to which they have access. Although the literature from practitioners is the most trustworthy, they are faced with the challenge of adhering to secrecy issues.

developed in Chapter 2, focusing on the elements indicated in Figure 12. The academic foundation of intelligence studies is discussed before a framework for understanding intelligence as a concept is compiled.



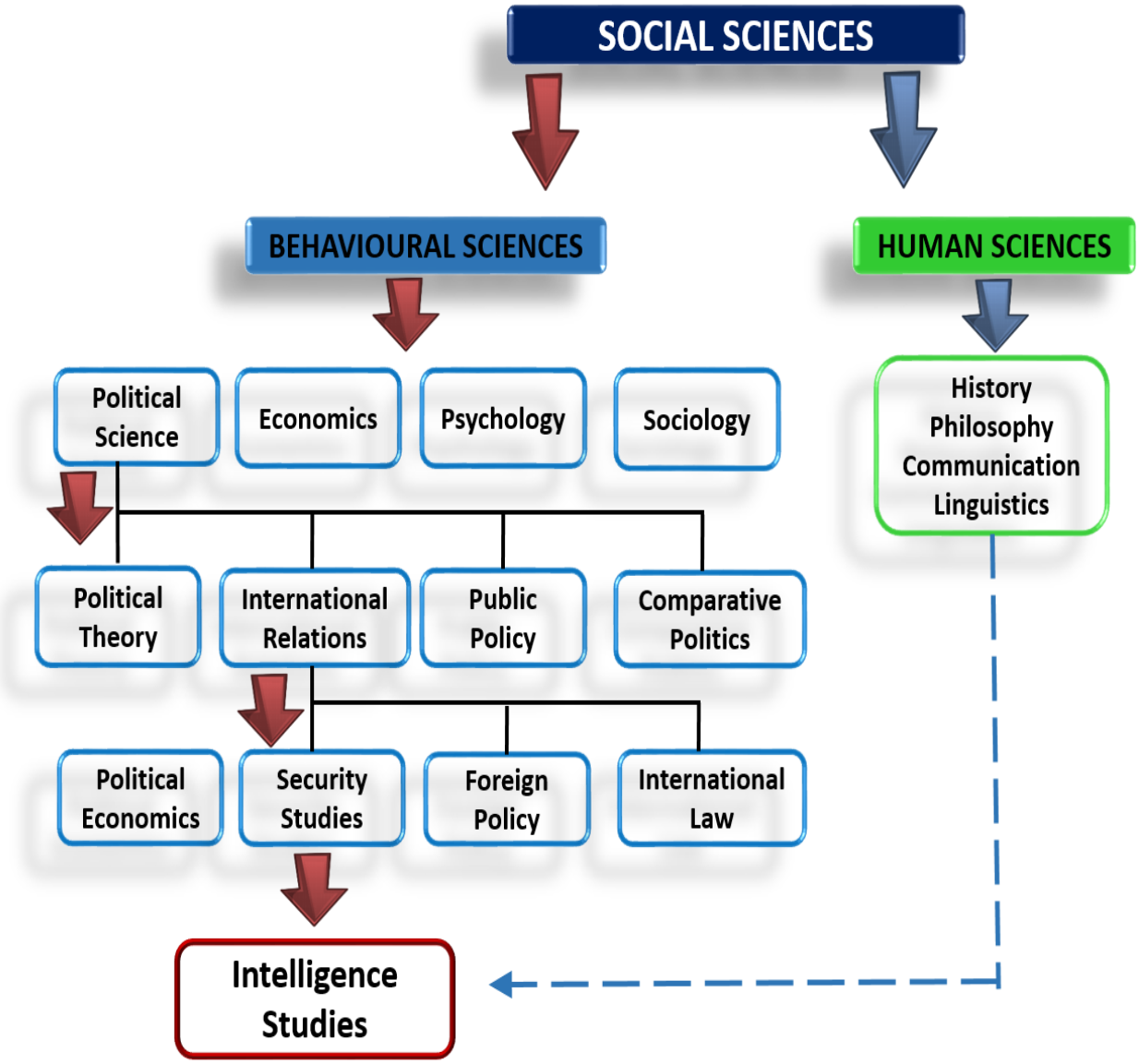
Source: Adapted from Duvenhage 1994:60; Greffrath 2015:29

Figure 12: Outline: Chapter 3

The chapter begins by explaining the academic links of intelligence studies with political science, international relations and security studies. These academic disciplines are unpacked in relation to their origins, definitions and relevance for intelligence studies. Security studies is discussed in more detail, as intelligence studies is a direct sub-field of this academic field. This section concludes with a discussion of the current state of the field of intelligence studies. The next section elaborates on conceptual frameworks within the field of intelligence studies; typology, models and theories, after which the concept of intelligence is discussed in detail. The chapter concludes with a conceptual framework for the intelligence component of SOCMINT that incorporates all the elements of social research applicable to this study.

3.2 Academic foundation of intelligence studies

This segment unpacks political science, international relations and security studies to highlight the academic origin of intelligence studies. It concludes with a discussion on the current situation within the field of intelligence studies. The academic linkages of intelligence studies are depicted in Figure 13. Intelligence studies is a behavioural science under the political science discipline and the sub-field of security studies (Figure 13). Although it resorts under behavioural sciences, it also has links to human sciences through the fields of history, philosophy and communication.



Source: Own construct

Figure 13: Intelligence studies

The first part of the next section focuses on political science and links to intelligence studies. Political science is viewed as one of the main disciplines within the behavioural sciences.

3.2.1 Political science and its links with intelligence studies

The origins of politics can be traced back to the classical Greek scholars such as Herodotus, Aristotle and Plato. The origin of the word *politics* is found in the Greek language, from the word *polis*, meaning *city-state* (Jackson & Jackson, 2003:22).

In the early development of the subject, it was studied as part of history, philosophy and law. It was only in 1880 that the first Department of Political Science was established in the United States at Colombia University (Jackson & Jackson, 2003:25). Even so, it was not until the 1930s that political science developed as a discipline. The development of political science can be divided into the following four periods:

- Traditional political science: This was the era from 1930 to 1960 and the main academic focus during this time was on formal governments and their legal powers. Studies were not informed by scientific methodology, as the perception was that social sciences do not have to be scrutinised as much as as natural sciences.
- Behavioural or empirical revolution: During the late 1950s, scientific research methods also found their way into the study of political science, especially in the form of empirical data collection. These methods enabled researchers to focus on and study human behaviour.
- Reaction to empiricism: During this time period, researchers were occupied with criticising the empirical movement within political science. One of the main criticisms against empirical studies was that the focus of research is more on quantifiable issues than matters related to public concerns.
- Period of accommodation: This period (since the early 1980s) saw scholars recognising each other's views and understanding scientific research within the political science discipline (Johnson *et al*., 2008:49–54).

Throughout this process, politics was a social activity that involved decisions relating to society. It is this characteristic that makes it difficult to define politics in a single way. Different political science scholars have their own perceptions and understandings of what this phenomenon entails. Heywood (2002:4) refers to political science as an "essentially contested" term. The Concise Oxford English Dictionary (2004:1110) has a broad definition

and describes politics as “the activities associated with the governance of a country or area”. Governance here refers to the establishment, implementation and monitoring of policies by the government within the jurisdiction of that particular country. According to Jackson and Jackson (2003:8), the following two definitions for politics are commonly accepted:

- The first definition is that of David Easton (cited by Jackson & Jackson, 2003:8), who views politics as “authoritative allocation of values”. Values refer to benefits and opportunities as anticipated by the people and “authoritative” implies a body responsible for this allocation.
- The second definition is “who gets what, when and how” by Harold Lasswell (cited by Jackson & Jackson, 2003:8).

Jackson and Jackson (2003:8) incorporate both these definitions and say that “politics embraces all activity that impinges on the making of binding decisions about who gets what, when and how”. Whereas the definitions of Easton (cited by Jackson & Jackson, 2003:8) and Lasswell (cited by Jackson & Jackson, 2003:8) focus more on the outcomes of governance, Jackson and Jackson (2003:8) manage to include all aspects related to governance (establishment, implementation and monitoring of policies). These definitions focus purely on what politics entails and not on the type of governance that is needed to implement the activities. For this reason, it is also important to highlight the types of government as the type directly affects the way intelligence is conducted in that country. This issue is discussed in detail in Section 3.3.1.

Taking all these definitions into consideration, politics for this study is the decisions made by a governing body regarding the optimal allocation of resources and the implementation and monitoring of these decisions. It is also important to mention that this study supports democratic principles with regard to governance.

With this broad description as background, it is imperative to highlight why intelligence studies is important to political science and how it fits into the discipline. This relation is based on political power and the protection of national interest. Power is always present where there is politics (Carr, 1946:102; Heywood, 2002:10; Jackson & Jackson, 2003:9). According to Jackson and Jackson (2003:10), this power can include anything from influence (the ability to persuade or convince others to either follow certain objectives or behave in certain way) to coercion (the opposite of influence that involves compliance by force). Governments have various instruments of power to their disposal to either influence or coerce individuals or other governments. Although instruments of power have long been part

of political science research (Edward Carr's *The twenty-year crisis 1919–1939: Introduction to the study of international relations* in 1939), intelligence was not always viewed as part of these instruments. Carr (1946:108–145) identified three instruments or categories of power within the political arena: military power, economic power and power over opinion. It was only recently that the National Defence University (cited by Worley, 2015:225) included intelligence as part of the instruments of power. These instruments include military, information, diplomacy, law enforcement, intelligence, finances and the economy, also referred to as MIDLIFE (National Defence University, cited by Worley, 2015:225).

In relation to intelligence, one of its most important functions is to protect national security. In this way, it could also be used as an instrument of power. This purpose is linked to one of the functions of government, which is to protect the citizens. In the case of South Africa, Section 41 of the Constitution (1996) states that the function of the South African government is to "secure the well-being of the people of the Republic". The intelligence community provides the government with timely, accurate and unique information regarding threats against and opportunities for the country. The government uses this information to formulate new policy or reformulate existing policy to address the issues at hand.

With regard to the South African context, the White Paper on Intelligence (1995:2) offers the following description of the purpose of intelligence:

- "To provide the policy makers, timeous, critical and sometimes unique information to warn them of potential risks and dangers."
- "To identify opportunities in the international environment, through assessing real and potential competitors' intentions and capabilities."
- "To assist good governance, through providing honest critical intelligence that highlights the weaknesses and errors of government."

For the purposes of this study, the White Paper's (South Africa, 1995:2) description is adopted as it clearly indicates the role of intelligence in the political process. Furthermore, this description is detailed and is applicable to both domestic and foreign areas of interest. In order to fulfil the purpose and to provide the policy maker with "timeous, critical and sometimes unique information to warn them of potential risks and dangers", all sources of information should be accessed. Currently, intelligence in relation to social media is not being used to its full potential. It is the aim of this study to put in place a framework that will

assist intelligence to use this important source of information, to enhance the collection process and ultimately the intelligence product.

This discussion elaborated on the academic links between intelligence studies and political science. The discipline of political science is divided into various sub-disciplines, such as international relations, political theory, public policy and comparative politics. The next section highlights the academic links between international relations and intelligence studies.

3.2.2 International relations and its links to intelligence studies

The sub-discipline of international relations is a relatively new discipline. International relations only gained recognition and support as a distinct discipline within the social sciences after the end of World War I when the Woodrow Wilson chair was established in 1919 at the University College Wales, Aberystwyth (Jackson & Sørensen, 2010:34; Wiener & Schrire, 2009:1). Although it has been recognised as a discipline, the exact nature and disciplinary character of international relations is still being debated today, as is evident in articles by Buzan and Little[15], and Baron[16] and Padmakumara[17]. This study subscribes to the notion that international relations is a sub-discipline of political science.

This sub-discipline studies relations and interactions between countries (on government level), and citizens and organisations outside the government structures such as non-governmental organisations and multinational corporations (Jackson & Sørensen, 2010:4). The global environment we find ourselves in is created by these relations among countries and other entities. An important aspect that needs some attention is the issue of non-state actors and the role they play and the influence they exert within the global sphere of international relations. According to the National Intelligence Council (2007:2), non-state actors are "non-sovereign entities that exercise significant economic, political or social power and influence at a national or international level". The role of non-state actors has always been minimal. However, the situation has changed over the past few decades as globalisation and technological development spread across the globe. The borderless environment creates a perfect situation for increased activities on the side of non-state actors.

---

[15] Buzan, B. & Little, R. 2001. Why international relations has failed as an intellectual project and what to do about it, *Millennium –Journal of International Studies,* 30(1):19-39.

[16] Baron, I. 2014. The continuing failure of international relations and the challenges of disciplinary boundaries, *Millennium – Journal of International Studies* 43(1):224-244.

[17] Padmakumara, S.C. 2014. The disciplinary identity of IR: an analysis on cross-disciplinary enterprise, *International Journal of Scientific Research and Innovative Technology* 1(5):83-92.

The study of international relations is even more necessary today where globalisation and the fast pace of technology development has created a world of ultra-high interconnectivity with no respect for state boundaries. This has a profound impact on international relations and on how business is conducted between countries. The current global environment has created ideal conditions for non-state actors to participate in activities, legal or otherwise. Non-state actors are increasingly playing an important role, especially in relation to international security issues. It is of importance that non-state actors also be included in the definition for international relations. For the purposes of this study, international relations is viewed as relations between governments, multinational corporations, multilateral organisations and non-state actors and the impact these relations have on the political and security environment within the country.

With this definition in mind, it is imperative to highlight how intelligence fits into the realm of international relations. Relations among governments also include, among other things, cooperation on intelligence issues. This cooperation takes place between intelligence organisations of the different countries and is governed by foreign policy objectives. Even though there has been intelligence cooperation among countries for a long time, it was not until World War I and II that this cooperation proved to be crucial. After the Cold War, cooperation increased to such an extent that Herman (1996:217) refers to “modern intelligence” as a “multinational activity”. Cooperation among the intelligence organisations of different countries includes information sharing on issues of common interest (such as terrorism, transnational organised crime), training of intelligence officers and a declared representative in embassies or missions in host countries. The intelligence officer serves as the nodal point for intelligence cooperation among countries.

In order to underline the role of intelligence with regard to international relations, it is important to refer back to the paradigm that was discussed in Chapter 2, labelled *interactive and interconnected*. One of the characteristics of this paradigm is the cooperation aspect. This includes cooperation across intelligence services on an international level. The new threats as a result of globalisation and a borderless environment have created a situation for the better use of this cooperation mechanism. International relations more than ever are about sharing information to address intelligence challenges and threats such as transnational organised crime and terrorism. Although state sovereignty and national interest remain at the centre, international safety is now also important and cooperation is necessary to ensure national and international security. The development of communication technology has enabled and amplified communication methods such as social media that do not adhere

to borders and the sovereignty of states. In this situation intelligence cooperation and information sharing is no longer optional, but an undisputable necessity.

Given these developments in international relations, the next important aspect in the academic origin discussion is security studies. The following section focuses on security studies as a sub-discipline of international relations, which is the academic basis of intelligence studies.

3.2.3 Security studies and its links to intelligence studies

Intelligence studies is at the core of this study and, as a direct sub-field of security studies (Figure 13), an in-depth analysis of the development of security studies is imperative.

In examining the field of security studies, it is apparent that there is no universal language in terms of defining security, the sub-discipline or the name of the sub-discipline. One of the most covered topics within the field is the "redefining of security" (Baldwin, 1997:5–26; Bellany, 1981:100–105; Rothschild, 1995:53–98; Ullman, 1983:129–153). However, this discourse has not produced a universally acceptable definition for security or for the name of the sub-discipline. This lack of agreement is clear in the terminology of the sub-discipline, which varies according to geographical area. In the USA, it is referred to as national security studies, while in the UK it is called strategic studies (Williams, 2008:3). Most literature refers to international security studies or security studies as the overarching term for the whole range of studies in security (Krause & Williams, 1996:229; Nye & Lynn-Jones, 1988:5). For the purposes of this study, security studies is used.

Security studies has its origins within the political science discipline under the sub-discipline of international relations. This academic field is specifically linked to western international relations relevant to nuclear weaponry and the Cold War (Baldwin, 1995:117; Buzan & Hansen, 2009:1; Griffiths & O'Callaghan, 2002:289; Williams, 2008:2). Although research and literature relating to war and peace strategies existed long before 1945 (Sun Tzu wrote *The Art of War* in 500 BC – Cleary, 1988), it is generally accepted that security studies as an academic field only emerged after World War II. This view is emphasised by Walt (1991:213) in his argument that prior to World War II, this field was limited to military contributions by professionals with a military background. During this period, civilian involvement was not acceptable or allowed. It was only during World War II that civilians became involved in military planning (Walt, 1991:213) through strategy documents and policy-related papers, laying the groundwork for the new field of security studies. In relation to the development of

this discipline, Shepherd (2013:xv) is of the opinion that Thomas Hobbes has been one of the most influential people, largely due to his writings on political organisation and social life in his book *Leviathan*[18]. She explains that "this book was the earliest expression of what became known as 'social contract theory', part of which was the theory that humans would agree to submit to the authority of a government as long as government provides them with security" (Shephard, 2013:xv).

It is of course important to define security as a concept. As mentioned previously, the field lacks a commonly acceptable definition for security. The concept of security has been described as an "essentially contested concept" (Williams, 2008:1), as "an underdeveloped concept" (Buzan, 1983:2) and a "powerful political tool" (Williams, 2008:2). Even though security has been widely used in the political science and international relations fields, the term has not been conceptualised. This begs the question why. In an attempt to answer the question, Buzan (1983:6–9) presents five reasons for this phenomenon. He starts off by mentioning that the term might be too complex; however, he also argues that this term is not less complex than power or peace, and therefore concludes that this is not an appropriate reason (Buzan, 1983:6). A second, and according to Buzan (1983:7) more conclusive reason for the lack of a definition for security, is that it overlaps with the term power. Within the realist model of the divided environment of the Cold War, the notion of international politics as a struggle for power never viewed the concept of security as a separate entity but rather as secondary to the concept of power (Buzan, 1983:6). As a result, academics were not compelled to explain and conceptualise the term because it was already implied in the term "power". Thirdly, Buzan (1983:7) mentions the opposition against the realist approach. It was mainly the idealists who rejected the realist approach by focusing on issues of peace (Buzan, 1983:7). The fourth reason is the fact that strategic studies is academically rooted in military strategy and defence studies (Buzan, 1983:7). Within the field of military studies, security is viewed very narrowly as a military term focused on war. Finally, Buzan (1983:9) points out that the practitioners of state policy are to blame for the lack of a common security definition. He explains that practitioners are of the opinion that it is in their best interest to "maintain its symbolic ambiguity" because it serves as a blanket for actions and policies that otherwise would need explanation (Buzan, 1983:9). Although Buzan (1983:9) mentions various reasons for the lack of a common definition, the author of this study is of the opinion that the military background of security studies is the biggest problem. The military view of security is confined to issues related to war and does not permit a broader view to include non-military issues. The fact that security studies had its origins during World War II (Walt,

[18] *Leviathan* or *The matter, forme or power of a Common-Wealth ecclesiasticall and civil* is a book written by Thomas Hobbes and published in 1651. In short the book is referred to as the *Leviathan*.

1991:213) makes it even more difficult to separate security from its war views and connotations.

In an effort to conceptualise the term various definitions are highlighted before concluding with a definition that best complements this study and its objectives. The definition of security varies from a narrow to a broad all-inclusive view. Bellany (1981:102) uses a very narrow definition and focuses purely on the military aspect in his description of security as "a relative freedom from war; coupled with a relatively high expectation that defeat will not be a consequence of any war that should occur". This narrow view on security creates problems as it ignores new security issues such as climate change, transnational organised crime and energy security, to name but a few. Ullman (1983:129) argues that in only focusing on military threats, other more harmful dangers are ignored and it also contributes to "militarisation" of international relations. The most basic understanding of security is being safe from harm or dangerous threats (Booth, 2013:xv; Griffiths & O'Callaghan, 2002:289). Even though this is a basic definition for security, it includes all threats and does not narrowly focus to one particular threat. In an effort to expand the definition, Ullman (1983:133) describes national security as "an action or sequence of events that (1) threatens drastically and over a relatively brief span of time to degrade the quality of life for the inhabitants of a state, or (2) threatens to significantly narrow the range of policy choices available to the government of a state or to private, non-governmental entities". This definition includes the previously mentioned threats and focuses on the effects of security issues on humans, which relates to human security, a new post-Cold War focus within security studies. The focus of security studies during the Cold War was on the state, security was closely linked to the theoretical assumption of the importance of the state (McSweeney, 2004:1–15). This situation has changed once again and currently the focus is on human security, especially if the wide range of non-military issues is taken into consideration. One of the advocates for human security is McSweeney (2004:14), who describes security as a "negative freedom". He follows a sociological angle and argues that the human perspective plays an important role in understanding international security, security policy and security in general (McSweeney, 2004:15).

With regard to the South African context, the White Paper on Intelligence (South Africa, 1995:3) also subscribes to the broad view of security: "Security in the modern idiom should be understood in more comprehensive terms to correspond with new realities since the end of the bipolar Cold War era. These realities include the importance of non-military elements of security, the complex nature of threats to stability and development, and the reality of international interdependence". The broader definition of security issues are of great

importance, especially to intelligence communities. Although some of the new threats have a smaller military component, it remains important to monitor as they have definite implications for national security.

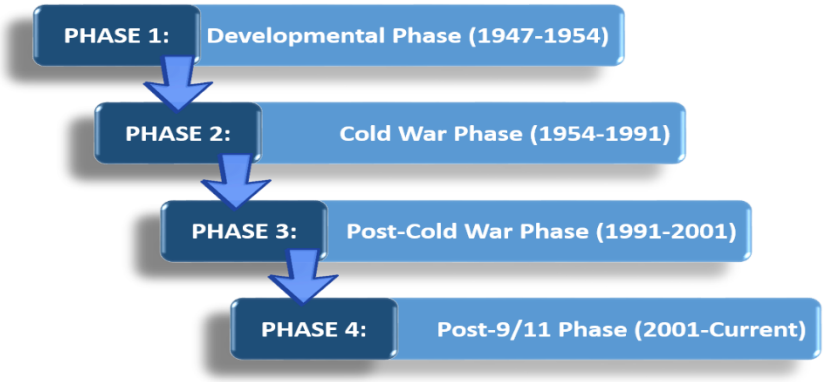
For the purposes of this study, the interpretation of the White Paper (South Africa, 1995:3) is adopted since it includes the non-military elements that play out in the international field and influence activities of intelligence organisations across the globe. Since the end of the Cold War the face of security and security threats have changed from a single threat model to a multi-dimensional model. During the Cold War, the arms race was the most important focus of intelligence organisations. However, since the end of the Cold War various new security threats have been identified. Some of these threats include terrorism, health pandemics, migration, energy security, cyber security, drug trafficking, money laundering, human smuggling and human trafficking. These threats have been exacerbated by globalisation, the fast pace of technological development and the appearance of non-state actors (mentioned previously) on the global arena.

With this brief discussion and clarification of what security entails, it is important to focus on security studies and its development. This serves as a precursor to the discussions in Chapter 5, where the history of intelligence is reviewed. As in the case of the term security, there is also no common understanding of what security studies entails. According to Buzan and Hansen (2009:8), there is no collectively accepted term for what international security studies encompasses. Williams (2008:2) concurs and explains that there are many diverse ways to reflect on security and security studies. Similar to the term security, security studies could be viewed in broad or narrow terms. Suchy (2003:12) views security studies in the broader sense as “an area focusing on a variety of threats and security aspects, not solely military ones”. This is in line with the wider view of what security threats entail. In contrast, Walt’s (1991:212) view is narrow and he perceives the occurrence of war as the most important target of security studies. In the same way, Baldwin (1995:117) also has a narrow focus and defines security studies as “the study of the nature, causes, effects and prevention of war”.

The definition of security should correspond with the study of the subject of security studies. Just as is the case with the concept *security*, it is vital to include all threats to national security in the academic field of security studies. For the purposes of this study, security studies is defined as the study of any threat that affects the national security of a country and its citizens. It is important to get an understanding of all threats that could affect the national

security and the well-being of the citizens. Therefore, all threats, military and non-military, should be studied.

The development of the sub-discipline of security studies is divided into four phases that started right after World War II, since it was during this time that national security became a central concern within international relations and this study relates directly to national security. The four phases are depicted in Figure 14 as the developmental phase, the Cold War phase, the post-Cold War phase and the phase after 9/11.



Source: Own construct

Figure 14: Phases in development of Security studies

The developmental phase of this discipline is the timeframe just after World War II (1947–1954). During this time, the international community was firm that such an event should never happen again. At this stage, the view on security was narrowly focused on military issues. In an effort to deal with this complex issue of national security, governments, especially in the United States, created new institutions such as the National Security Council to deal with the administration and management of the issue (Bock & Berkowitz, 1966:122). This was the start of institutional growth within the security sector, which can be viewed as the pioneer for the current intelligence services. This development can also be regarded as the main contribution of this phase.

The second phase was the time during the Cold War (1954–1991). During the Cold War the study of security increased substantially and the primary focus was on “strategic relations among states” (Booth, 2013:xv). During this phase, security studies was characterised by three distinct timeframes: the “Golden Age” (Walt, 1991:213) from 1954 to 1966, the Vietnam War (1 November 1955 – 30 April 1975) and its aftermath, and then the “renaissance” period from 1970 to 1991. The first timeframe was labelled the “Golden Age” because of the surge

in academic research in the field, especially in relation to the nuclear revolution phenomenon (Walt, 1991:214). The “golden age” was followed by the Vietnam War. This was a period of decline. Academically the feeling was that the research programme under the rational deterrence paradigm was fully understood (Baldwin, 1995:124; Walt, 1991:216). After the Vietnam War, the field experienced a “renaissance”, according to Walt (1991:220). He highlights the following reasons for the new interest in the field of security studies:

- By the end of the Vietnam War, security studies was no longer obsolete, especially if the focus was on understanding history and gaining knowledge from historical errors.
- The collapse of *Détente*: The deterioration of relations between the USA and the Soviet Union increased international tension, which amplified the interest in this field.
- Increased access to data: Previously restricted data were made available in the public domain and this created a good environment for productive studies relating to security issues.
- Increased outlets for publishing: Various journals were launched during this time period and this created a good environment for producing articles for peer review. Some of these journals include *International Security* (1976) and *Journal of Strategic Studies* (1978).
- Financial support: The access to information raised public awareness about national security issues within the United States of America, resulting in increased financial support to various institutions dealing with security studies.
- Security studies and social science: Security studies adopted the norms and objectives of social sciences in relation to theory creation, theory testing and theory application. (Walt, 1991:220).

All these developments worked together to create the renewed interest in the field, or a “renaissance” as Walt (1991:220) termed it. What is of importance during this timeframe is the increase in data and information. This is also the time during which the development of technology (see Chapter 7), specifically the creation of the internet, increased the amount of data and the access to the data and information. Throughout this timeframe intelligence was narrowly focused, intelligence priorities were fixed and intelligence organisations knew exactly what was expected.

The third phase is the post-Cold War phase (1991–2001). Within the field of international politics, the end of the Cold War is perhaps one of the most important events since the end of World War II (Baldwin, 1995:117). This new era in international politics has also

influenced the field of security studies. During the Cold War, security was well defined and understood. However, the globalisation effect has resulted in a change in the scope and policy related to security issues, looking more broadly, not only nationally, but also regionally and internationally. According to Kristensen (cited by Cavelty & Mauer, 2010:4), "achieving absolute security is no longer possible". This implies that states have moved from being either "secure or not secure" to "never secure" and they need continued risk management on a national, regional and international level (Cavelty & Mauer, 2010:4). Globalisation over the past six decades has changed the global environment in such a way that the world has become borderless, interconnected and co-dependent. This is also the case with security-related issues. The new environment also forces governments in general and intelligence communities in particular to re-look the concept of security and security issues[19]. It is important to note that intelligence communities have lagged behind, specifically in relation to communication technology and its impact on security (NSTI, 2012:1). The most important development during this time was the broadening of the security agenda to also include non-military issues. This implies that intelligence organisations had to re-look and re-align priorities to include new security issues such as energy security, food security, environment security and transnational organised crime.

The fourth phase is the phase after 9/11 (2001–current). According to Cavelty and Mauer (2010:2), security studies is currently one of the most "dynamic areas of international relations" mainly as a result of the 9/11 attacks and the subsequent *Global War on Terror* campaign by the USA. Since 9/11, terrorism has shot to the top of the security priorities in various countries across the globe. The debate on the widening of security issues escalated even further after 9/11 and is being shaped by world developments. This is leading to an ever-increasing list of security issues and includes issues related to population movements and human security.

When analysing the phases, it is apparent that the most significant development and academic contributions within the field of security studies took place during the post-Cold War period, continuing into the phase after 9/11. These developments are also relevant to the progress of intelligence studies especially in relation to the widening of the security agenda. Since the end of the Cold War, the security environment has changed with regard to

[19] One of the most important issues in relation to security studies since the end of the Cold War has been the debate about the widening of security issues. Views within the field of security studies can be divided into two main groups: the wideners (expanding of the security agenda to include various non-military issues) and the traditionalists (military and state-centred issues) (Buzan *et al.,* 1998:2).

the scope of threats to national security. The widening of the security agenda directly affects the focus and priorities of intelligence services.

This section explained the academic roots of intelligence studies, inter alia political science, international relations and security studies. This creates a good understanding of the academic origin of intelligence studies. Furthermore, it serves as an introduction to the next part of this chapter, which focuses on intelligence studies as academic field.

3.2.4 Intelligence studies as academic field

As mentioned previously, intelligence studies is a very young academic field of study and its development has been slow. This is a result of the lack of archival access because of secrecy and the lack of transparency during the early developmental stages (Wark, 1994:1). However, this situation changed in the mid-1970s[20] after investigative journalism into events in the United Kingdom and the USA resulted in increased transparency in relation to aspects of intelligence (Wark, 1994:1). This transparency opened up access to historical data and archives previously not in the public domain and academic scholars outside of the intelligence environment started to study and write about the phenomenon of intelligence. This caused the "intelligence revolution" which led to the "scholarly revolution" in the last quarter of the 20th century (Wark, 1994:2). Marrin (2014:14) refers to this time as the "formative stages" of intelligence studies. During this time, there was a substantial increase in courses in intelligence studies and an increase in articles on the subject in journals such as *Intelligence and National Security, Intelligence and counter intelligence* and the *International Journal of Intelligence*. The focus of writings and studies can be divided into intelligence projects, research projects (primary source documentation), historical projects, case studies, definitional projects, paradigm projects, methodological projects, journalism projects and popular culture projects (Gill & Phythian, 2012:6; Thomas, 1988:236; Wark, 1994:2–7).

Even though there has been an increase in academic interest and writing in the field of intelligence studies, growth in the theoretical foundation has been lacking. Kahn (2001:79) indicates that even though various authors refer to their work as "theory of intelligence", no one has proposed concepts to be tested[21]. Marrin (2014:1–2) concurs and is of the opinion that although intelligence studies literature and the interest in the field is growing, there are

[20] Revelations of "Ultra Secret" and code breaking capabilities and successes of the Allied forces during World War II.

[21] As mentioned in Chapter 2, a good theory should be testable.

“significant gaps in the literature due to generalised failure to ensure knowledge accumulation and aggregation over time”. Walsh (2011:288) agrees and argues that a “discipline of intelligence cannot develop unless research can be generated in a coherent way that has impacts applicable to industry partners”. In Chapter 2 (2.4.3), six criteria for a discipline were highlighted. When comparing intelligence studies to these criteria, it is clear that it cannot be classified as a discipline yet, the main reason being that even though intelligence studies has a specific research focus (intelligence) its “body of accumulated specialist knowledge” and theories and concepts are inadequate.

In order to grow it into an academic discipline there is an urgent need to build on existing theories and knowledge. In an effort to improve intelligence as a discipline, Marrin (2014:1) underlines a need for reinforcing best practices such as identifying, acquiring, storing, creating and disseminating new knowledge. Marrin (2014:10) describes these steps as follows:

- recording the known;
- identifying gaps;
- working to address the gaps;
- distribution of knowledge to the client (government); and
- institutionalising these actions.

However, Gill and Phythian (2012:15) raise two major challenges facing intelligence studies that affect the growth of this academic field. The first challenge is the continued domination of Anglo-American literature (Gill & Phythian, 2012:15). There is an urgent need for literature from other communities to balance the global intelligence picture to avoid Anglo-American experiences being imposed on other countries. New and alternative literature and theories are needed to prevent imposing experiences on countries with different environments and different levels of development. This will also assist in increasing the knowledge base of intelligence studies and comparative studies can then be undertaken. The second challenge is the mistrust between academics and practitioners within the field of intelligence (Gill & Phythian, 2012:15). The declassification of secret documentation after the Cold War ensured the involvement of academics in the field of intelligence. This involvement has played a crucial role with regard to the increase in intelligence studies literature. This underlines the fact that academics do have a role to play in terms of their academic expertise and building of especially the theoretical base of intelligence studies. Closer cooperation between academics and practitioners is crucial for the development of this academic field.

This section had the main purpose of explaining the academic origins and links of intelligence studies. It is important to clarify these links as it provides a basis for the conceptualisation of intelligence. Furthermore, it provides clear pointers with regard to history, theories and paradigms for understanding the field of intelligence studies. As explained, intelligence studies originates within the discipline of political science and plays a crucial role with regard to policy making. The next academic link of intelligence studies is international relations, which is a sub-field of political science. Intelligence performs an important role with regard to diplomacy in the form of liaison with other countries. Security studies, a sub-discipline of international relations, completes the intelligence studies academic hierarchy. For the purposes of this study, intelligence studies are viewed as an academic field belonging to the sub-discipline of security studies.

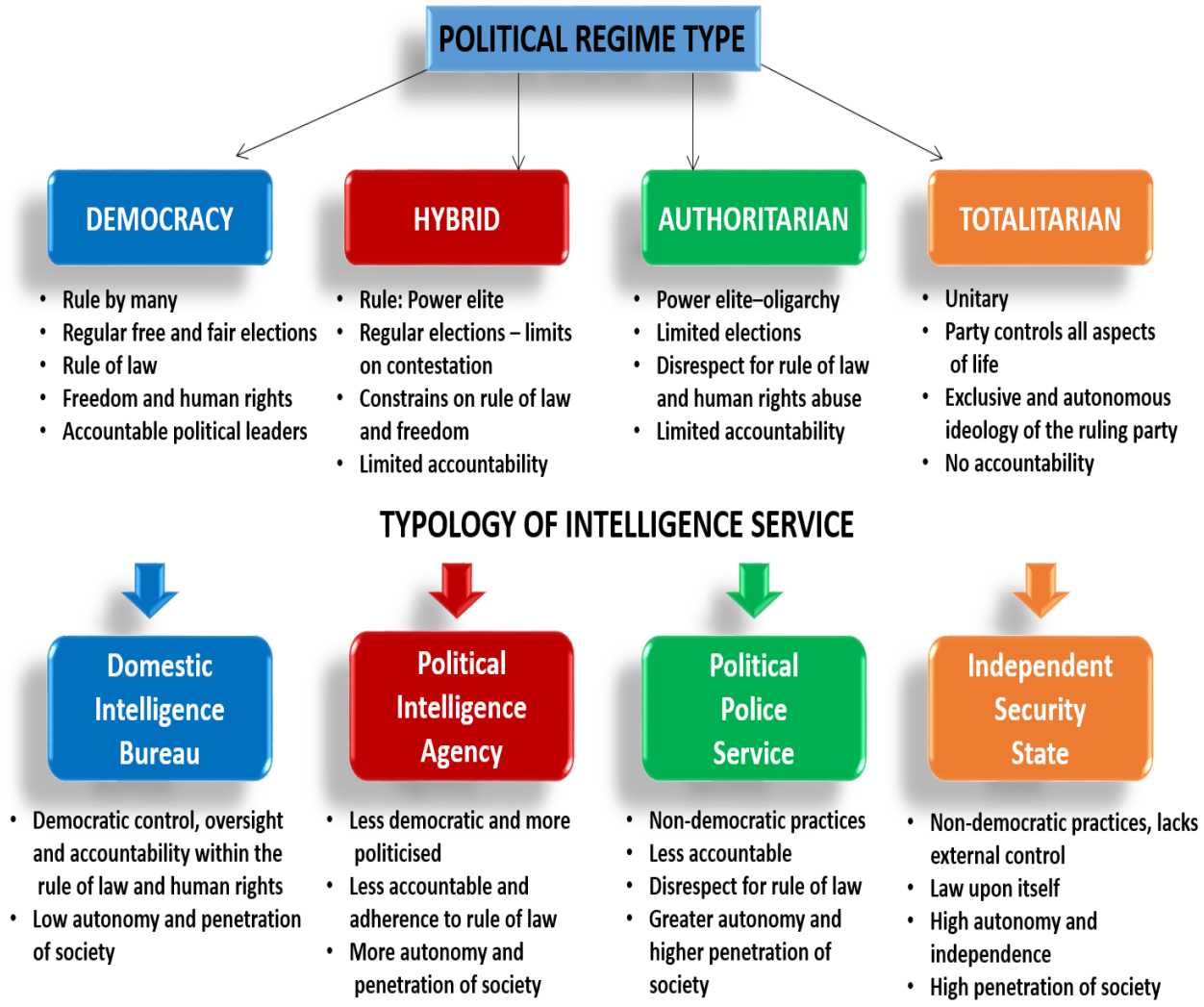
The next elements of the conceptual framework are traditions and paradigms. However, these elements were discussed in great detail in Chapter 2 and the reader is referred to Section 2.4.4 and 2.4.5. Therefore, the next section focuses on conceptual frameworks within the field of intelligence studies.

3.3 Conceptual frameworks within intelligence studies

Chapter 2 has already provided detailed information on conceptual frameworks and its applications in social science research. This discussion focuses on conceptual frameworks within the field of intelligence studies. It is divided into three sections to address three conceptual frameworks: typology, models and theories.

3.3.1 Typology in intelligence studies

In today's political environment, all governments have an intelligence service. Bruneau (2001:337) is of the opinion that countries cannot afford to be without this function. According to Hutton (2007:2), the activities of the intelligence community is determined by the political environment within the country. The typology of the intelligence services therefore runs along the same lines as the typology of the political system within the country. Van den Berg (2014:77) identifies four types of intelligence services in his typology: bureaus of domestic intelligence, political intelligence agencies, political police services and independent security state services (Figure 15).



Source: van den Berg, 2014:78

Figure 15: Typology of Intelligence Services

Van den Berg (2014:78) links four political regime types to four different types of intelligence services: a democratic regime is linked to a domestic intelligence bureau, a hybrid state would have a political intelligence agency; an authoritarian regime would have a political police service; and a totalitarian state would have an independent security state type of intelligence service. These organisations differ in relation to the level of democratic control, accountability, adherence to rule of law, autonomy and penetration of the society they serve. In relation to the South African context, I refer to Van den Berg's (2014:172)[22] study, which concludes that South Africa can be classified as a hybrid regime with a political intelligence

[22] For a detailed discussion on this matter, Van den Berg's *The intelligence regime in South Africa (1994-2014): An analytical perspective* provides excellent insight into the matter.

agency structure. The characteristics of the political intelligence agency are set out as follows:

- The intelligence structures reflect practices from both democratic and authoritarian regimes – hybrid.
- It is more politicised and serves the ruling party and the political elites linked to the ruling party.
- The focus of the intelligence services is on the opposition parties and threats to the ruling party and not on the protection of the constitution, well-being of the citizens or the security of the country as a whole (Van den Berg, 2014:172).

When evaluating the South African situation against these characteristics, it is clear that the intelligence organisations can be classified as political intelligence agencies.

Since the typology of the intelligence services is closely linked to the political regime within the country, examining the political regime makes clear how the intelligence service would view democratic control, accountability, rule of law, autonomy and penetration within society. For the purposes of this study, South Africa is classified as a hybrid state with an intelligence service that is less democratic, more politicised, less accountable and more independent. Previously it was indicated that the scope of security threats has increased after the end of the Cold War. This situation has necessitated a shift in intelligence focus. However, in a political intelligence service this proves to be difficult as the focus is on party threats and party interests. Threats to national security are only entertained if they are also a major threat to the party. Resources might not be available to shift the focus to issues threatening national security.

With this clarification of typology as background, the next element of the conceptual framework relevant to this study is models. The next section focuses on the issue of models in detail.

3.3.2 Models in intelligence studies

One of the most used models within intelligence studies is the intelligence cycle (Figure 16). Hulnick (2006:959) is of the opinion that “no concept is more deeply enshrined in the literature than that of the intelligence cycle”. The cycle elucidates the intelligence process, which comprises the elements or functions of intelligence. These elements are combined

into a model that explains the order of activities that collects, produces and delivers intelligence to the decision maker (Johnson, 2009:34). The elements include requirements (planning and direction), collection, analysis and production, dissemination and feedback (Johnson, 2009:34; Lowenthal, 2006:54). Lowenthal (2006:54) also refers to the intelligence process as the “steps or stages” of intelligence.

Source: Adapted from Lowenthal, 2006:65

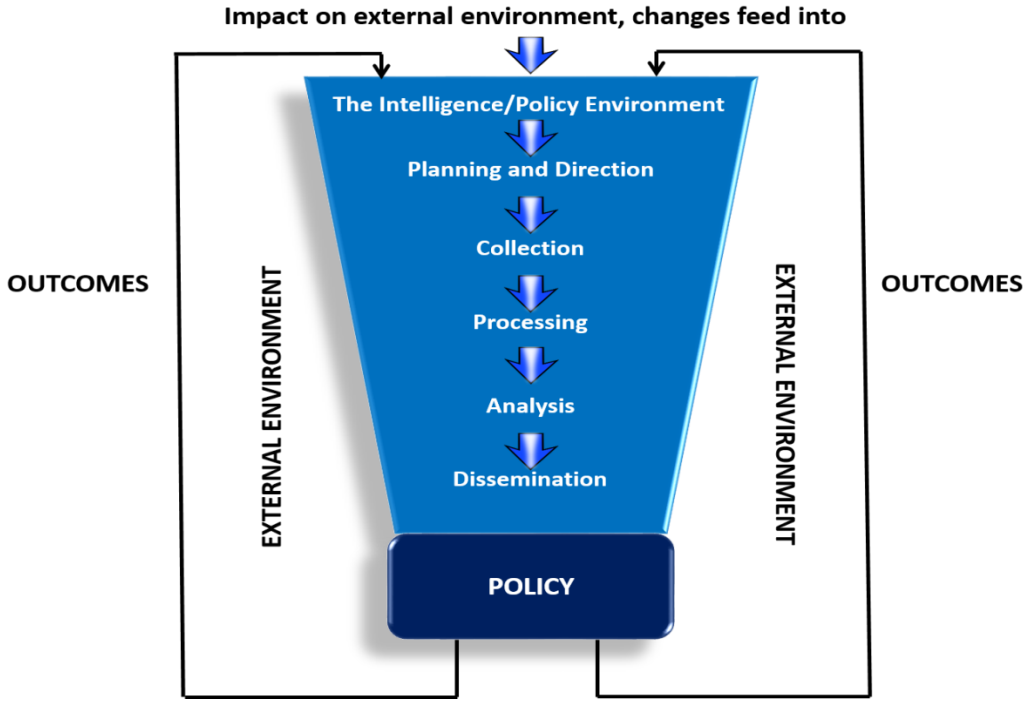
Figure 16: Intelligence cycle

The use of the intelligence cycle to explain the intelligence process is widely debated and various views exist. Gill and Phythian (2006:3), Lowenthal (2006:66), Clark (2013:5) and Hulnick (2006:959) are of the opinion that the intelligence cycle is not a suitable way to describe the intelligence process. However, they provide different reasons for their observation. According to Hulnick (2006:959), the cycle is a “flawed model” for the following reasons:

- The client rarely gives collection guidance: Guidance in terms of requirements usually comes from within the organisation. The process of identifying the gaps in the intelligence picture drives the intelligence process, not direction from the policy maker. The process of identifying gaps in the information picture is usually done by the analyst who has an overall idea of the available information. These gaps are then communicated to the collection arms for further investigation and clarification.

- Collection and analysis work in parallel rather than in tandem: Raw unevaluated information goes to the analyst and to the policy maker at the same time. This practice is problematic as raw information should be evaluated and contextualised for it to be useful to the policy maker. Raw information can be misinterpreted if not contextualised. This could have major implications with regard to policy issues.
- Intelligence supports and does not inform policy decisions: One of the purposes of intelligence is to assist policy makers in policy decisions. However, in many cases decision makers use intelligence to affirm decisions already made.
- CI and covert action is not part of the cycle: It is especially CI that is of great importance to safeguard a country against espionage.

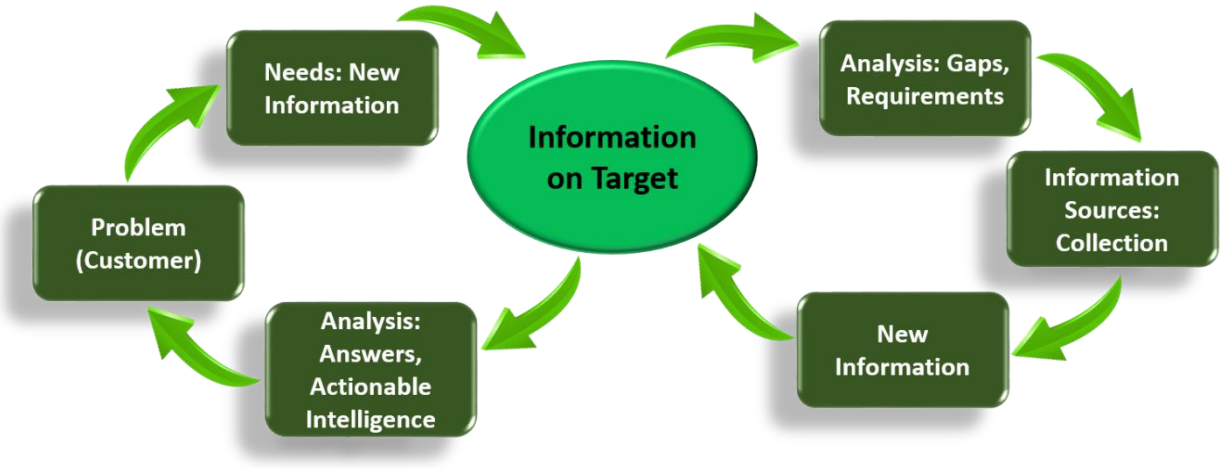
Gill and Phythian (2006:3) on the other hand argue that the cycle cannot describe the interactivity of intelligence with the client and the external environment. They describe it as a funnel (Figure 17) where not all information is translated into policy through analysis, it is filtered out until only the necessary information is used for policy formulation (Gill & Phythian, 2006:3). Interactivity between the intelligence organisation and the client is of great importance. The new technological developments allow for this process to take place on a regular basis and within a secure environment. Information is immediately available for distribution and face-to-face interaction is possible with the use of technology such as Skype or webinars.



Source: Adapted from Gill & Phythian, 2006

Figure 17: The intelligence process

Another critical evaluation of the intelligence cycle originates from Clark (2013:5). According to Clark (2013:5), the intelligence cycle is almost a “theological concept”, which does not work. However, the intelligence community continues to use it because it fits the conventional paradigm of problem solving. He provides two reasons why the intelligence cycle is not a true reflection of the intelligence process: because of the “silofication” of each activity the quality of the final product is compromised; and, the feedback from the client to the intelligence community is absent (Clark, 2013:5). The client does not always have time to provide the intelligence community with feedback. In order to address these issues he proposes a target-centric process that includes all stakeholders (Clark, 2013:7–8). This approach underlines the sharing of information and each entity extracts the necessary information from the pool of information known about the target (person or organisation) to do their job. Once new information is received, it is fed into the system for everybody to observe and use. The process is explained in Figure 18 below. This process supposes a central database from where information is deposited and accessed. All relevant intelligence officers with necessary clearance will have access to the same information and everybody will work from the same departure point.

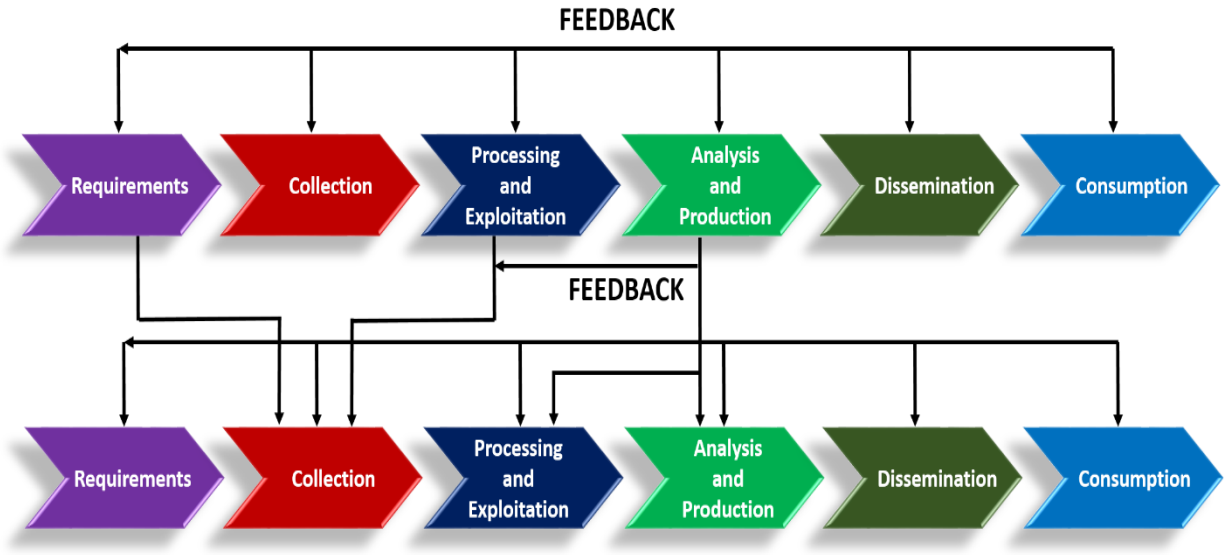


Source: Adapted from Clark, 2013

Figure 18: Intelligence as a target centric process

Lowenthal (2006:66) also provides an alternative to the intelligence cycle. He describes the traditional cycle as “uni-dimensional”, which does not accommodate any random situation that might occur from time to time (Lowenthal, 2006:66). He argues that the intelligence cycle does not include feedback and that the process might not be finalised within one cycle.

He therefore proposes the "multi-layered" process that is "linear, circular and open-ended at the same time" (Lowenthal, 2006:66–67). This process is depicted in Figure 19.



Source: Adapted from Lowenthal, 2006

Figure 19: Multi-layered intelligence process

One of the most important features of this multi-layered process is that it allows for feedback during any time of the intelligence process. For example, once the analytical process starts and gaps are identified, feedback can immediately be provided to the collection process. Although this practice does take place within the intelligence environment, the traditional intelligence cycle does not cater for this. Feedback is an important way to guide the collection process to obtain relevant information. Various processes take place with regard to the same requirement and the traditional intelligence cycle does not take these activities into account. Closer and more regular cooperation and interaction with the client will also assist in providing correct information.

Although the idea of a cycle is being debated and new proposals have been made, the traditional cycle of intelligence is still applied within intelligence services around the globe, even within the South African intelligence environment. However, this study supports the "multi-layered" approach. This best describes the intelligence process, which is not a cycle, but an open-ended linear[23] procedure with the possibility of feedback throughout the whole process. This is a more realistic approach to the intelligence process as it allows for a return to a previous step for clarification or for collecting more information. Feedback is of great

[23] While a traditional linear process does not allow for feedback, the multilayered linear approach (depicted in Figure 19) provides the opportunity for feedback and response.

importance in this model, not only feedback from the client, but feedback throughout the intelligence process. This model focuses on guiding the intelligence process to reach the correct outcome through constant interaction between all the steps of the process. Nevertheless, it is doubtful whether the client (government) will provide feedback and indicate the usefulness of products due to time constraints.

With the typology of the intelligence services and the model of the intelligence cycle clarified, the final element of the conceptual framework, namely theory, is discussed in the next section. All three these frameworks form the sixth element of social science research and intelligence studies in particular.

3.3.3 Theoretical approaches to intelligence studies

Before drilling down into the discussion of the different theories applicable to this study, some perspectives should be contextualised to inform the discussion on theory.

These perspectives include the following:

- All theories of intelligence studies can be traced back to Sherman Kent's *Strategic intelligence for American world politics* (1949). However, the fact that that there is no established definition for intelligence limits the development of theories within this field (Marrin, 2014:5).
- Certain principles are relevant to the study and theory of intelligence. Kahn (2001:84-86) describes three such principles. The first principle relates to the function of intelligence and holds that "successful intelligence optimises one's resources" (Kahn, 2001:84). Although Kahn (2001:84) applies this principle to military actions, it is also relevant to civilian intelligence activities. Correct intelligence about the position of the opposition party/country could lead to a positive outcome during a negotiation process. The second principle Kahn (2001:84) mentions is that it "is an auxiliary and not a primary element in war". This implies that intelligence serves or assists war activities although it is not physically part of the war. In relation to the civilian intelligence services, it implies that it will increase the probabilities of a positive outcome. In the previous example of negotiation, it will serve the negotiating team and assist in reaching the desired outcome. The final principle Kahn (2001:85) refers to is that "intelligence is essential to the defence but not to the offence". This might be true with regard to the military and the winning of battles. However, in today's age of cyber warfare the offence is as important as the defence, especially with regard to safeguarding information. Van Solms (2014) notes that

to survive in today's cyber war environment defence is not adequate, there is a need to "fight back" and therefore a need for a good offence.

- Intelligence in essence is concerned with human interaction and this reality creates opportunities for intelligence services to obtain information. Johnson (2009:33) argues that the starting point to a theory of intelligence should be human nature, and in particular two dominant motivations: survival and prosperity. He applies it to the level of national government, which seeks information about threats (survival) and opportunities (prosperity) for national security.
- Within intelligence, there are theories for (from academics outside intelligence) and theories of intelligence (practitioners from inside intelligence). Gill (2006:4) argues that there should not be a distinction between theory "for" and theory "of" intelligence – "a good theory of intelligence (to assist academics research intelligence) should, by definition, be useful for intelligence" (practitioners of intelligence). Although the end goal of practitioners and scholars is different, both will benefit from being theoretically grounded. Scholars focus on understanding and gaining knowledge that will stand up to scrutiny of peer review while practitioners should provide a report with knowledge that is actionable by the client.

The next section focuses on the theoretical approaches. Various theoretical approaches to the field of intelligence studies are available, but this study is best served by realism as a traditional approach and postmodernism as a relatively new approach.

Realism is the most popular approach within the security field in general and intelligence studies in particular. Phythian (2009:57) is of the opinion that structural realism is the "explanatory approach to international relations most centrally concerned with security". This implies that structural realism already provides a theoretical base for issues such as the importance of intelligence. The discussion now turns to the features of realism and the specific characteristics related to structural realism in intelligence.

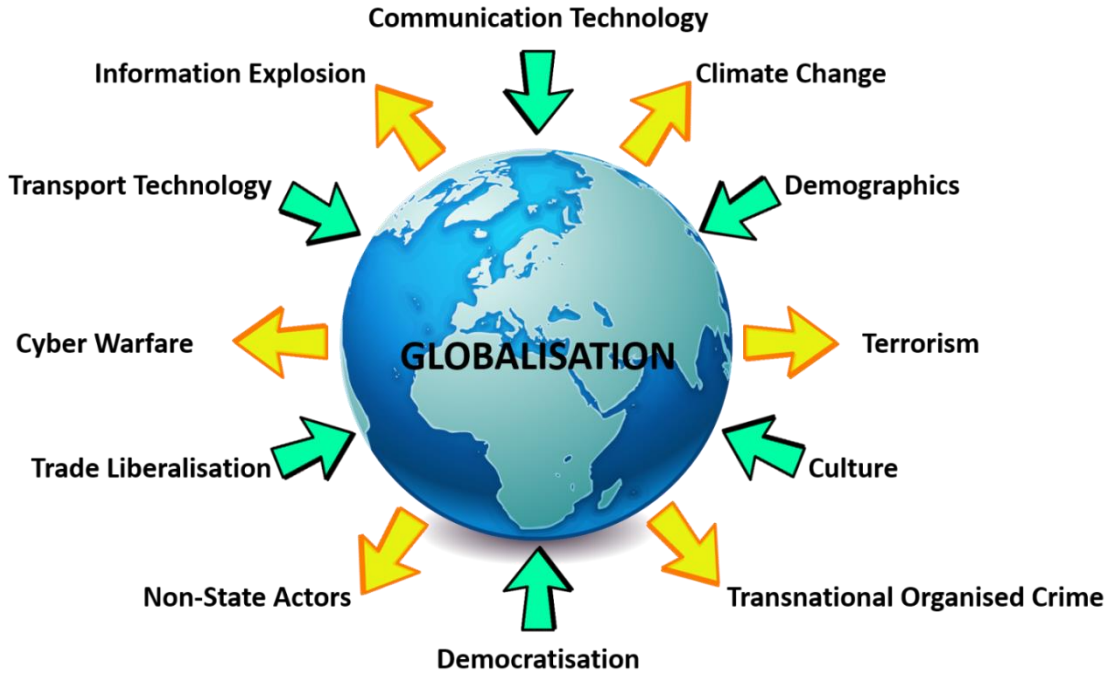
Realism consists of different variations. However, there are basic characteristics shared by all variants (Collins, 2013:14). These characteristics include the following:

- The most important feature is that the international system lacks a central authority and is therefore described as anarchic; implying that within this international system there is no single authority that can avert the use of force or enforce treaties (Glaser, 2013:14; Hay, 2002:18–19; Jackson & Sørensen, 2010:66). Therefore, according to Jackson and

Sørensen (2010:66), the "normative core of realism is national security and state survival" and foreign policy primarily aims to advance and defend the interest of the state. Consequently, each state is on its own to ensure its survival by its own means. This implies a military capability and intelligence services with national security as its main priority.

- Power is crucial in realism (Glaser, 2013:14; Heywood, 2002:128; Hay, 2002:18–19). Here power refers to a state's ability to build military capacity. The more a state's capacity (wealth, technology and human resources), the more powerful it is, posing a bigger threat to other states. This is also an important feature of structural realism within intelligence. International politics is dominated by power and the main role players are "great powers" concerned with "power politics". In the international political arena, states are always cognisant of the situation of another state's economic, political and military power (Hay, 2002:18–19; Phythian, 2009:57; Mearsheimer, 2007:71; Söderblom, 2004:21).
- States are viewed as unitary entities (Hay, 2002:18–19; Glaser, 2013:14).
- States are regarded as rational actors and decisions are made by balancing their needs or interests with their capabilities (Hay, 2002:18–19; Glaser, 2013:14).
- States evaluate other states in terms of power and capabilities and react accordingly (Glaser, 2013:14). With regard to structural realism, security and order is the priority of the state – war is the last resort after "deterrence has failed" (Mearsheimer, 2007:71; Phythian, 2009:57; Söderblom, 2004:21).
- The state remains the key factor and the only referent object within the international system. International institutions play a less significant role (Glaser, 2013:14; Hay, 2002:18–19; Mearsheimer, 2007:71; Phythian, 2009:57). This implies that the state is the main role player in international politics and international security, which leaves no room for non-state actors.
- States operate within a global system of competition and war (Glaser, 2013:14; Hay, 2002:18–19). Structural realism also underlines this feature. The competition among states together with the uncertainty of the objectives of other states within the international arena emphasises the importance and need for intelligence (Mearsheimer, 2007:71; Phythian, 2009:57; Söderblom, 2004:21).
- State survival and national security drive foreign policy (Jackson & Sørensen, 2010:67). This underlines the earlier discussion (see section 3.2.1) of intelligence as an instrument of power within the political arena. It implies that there is a definitive role for intelligence in relation to foreign policy and the safe-guarding of national security.

These characteristics underline the reason behind the popularity of realism within intelligence studies. However, the global context has changed since the end of the Cold War. Haynes *et al*. (2017:7) argue that the increased interaction between international role players (as a result of globalisation) has made the distinction between domestic and foreign policy unclear. This situation results in an increase in the scope of international relations and equally in the scope of security studies. This new security environment brought about by globalisation is characterised by a borderless, highly interconnected and inter-related world that needs a broader and deeper security agenda.[24] What's more, Booth (1991:314) argues that the expression "post-Cold War era" does not capture the full extent of the changes that have taken place and trends that are evident since the end of the Cold War. It is imperative to explain the changes and globalisation since the end of the Cold War. The main drivers of globalisation include the continued development of communication technology, improvement of transport technology, demographics and movement of people, spread of different cultures, spread of democratisation and trade liberalisation (Figure 20). These drivers have an impact on domestic situations within countries. This necessitates domestic and foreign policy formulation and redirecting in relation to issues of national security.



Source: Adapted from the National Intelligence Council, 2012

Figure 20: Drivers and security trends of Globalisation

[24] The broadening includes non-traditional security issues such as energy security, counter-terrorism, food security, water security and environmental security, among others (Booth, 1991:318, 319; Irondelle, 2013:4; Krause & Williams, 1996:229). There is an expanded focus on the referent object beyond the state to include non-state actors (Booth, 1991:318, 319; Irondelle, 2013:4).

Some of the security trends resulting from globalisation are depicted in Figure 20. These include information overflow, climate change, terrorism, transnational organised crime, an increase in activities of non-state actors and cyber warfare (Booth, 1991:314; Collins, 2013:289–379; Krahmann, 2005:4). These realities have led to the erosion of the sovereignty of the state and a weakening of the military element of security. In this regard the US Director of National Intelligence, McConnel, wrote: "We are engaged in a dynamic global environment, in which the pace, scale and complexity of change are unprecedented. It is a networked world where what happens in Peshawar affects Peoria, and vice versa. Risks are often unforeseen and threats are hidden and agile, making the job of intelligence professionals more critical and more challenging. Our national security depends on anticipating risks and out-manoeuvring our adversaries, not just out-muscling them. Therefore, intelligence is more critical than ever" (National Intelligence Council, 2012:1).

This reality is not only true for the USA, but for intelligence organisations across the globe. Intelligence communities are faced with numerous drivers currently shaping and influencing the global security environment, intensifying uncertainty and increasing the need for intelligence. The new global security environment has certain implications for the intelligence community in that geographical and jurisdictional borders are blurred, distinguishing between intelligence and non-intelligence issues are complex and lines between domestic and foreign policy issues are unclear. Even though the threat has broadened to include a variety of issues that were previously not seen as traditional security issues, the truth is that the intelligence community did not stay in touch with the changed environment. Most intelligence agencies still conduct intelligence as they did during the Cold War (NSTI, 2012:1).

It is clear that all these trends and changes have implications for theorising across disciplines. It is important to realise that issues cannot be studied in the same way they were during the Cold War and existing theories should be relooked. In spite of these new realities, realists such as Waltz (1979:39) continue to believe that realism remains an important theory in international politics. The only way realism will no longer be relevant is when the world has been "transformed" and the international political system is no longer dominated by states (Waltz, 1979:39). This implies that the state is no longer the referent object in international politics. According to Waltz (1979:39), this has not happened, "the structure of international politics has simply been remade" by the ending of the Cold War. However, it remains the conviction of this study that although states remain important role players within the international political arena, non-state actors also have to be taken into account as their activities have enormous implications for international security.

Theories should be adapted and changed to find a new way of explaining global phenomena. This is true for political science, international relations, security studies and intelligence studies. This new focus of the security agenda creates problems for realism, especially with regard to the referent object. When referring to all the new security issues and the borderless environment, non-state actors have a significant impact on global security. Traditional theories do not address and explain the new global environment and the subsequent new security challenges adequately. There is a need for a new way of looking at and analysing security-related phenomena. The current security situation is characterised by a borderless environment in which non-state actors play a crucial role. Intelligence organisations find it hard to adapt to the new security environment as they are still operating within Cold War parameters.

It is against this background that postmodernism is proposed as a new approach to intelligence studies. The world we live and operate in is not a static environment, it changes, and this is happening at an increasing pace. This implies that especially governments and their departments should also adapt to these changes in an effort to continue to be effective. This is also true for intelligence organisations. These organisations have particularly been influenced by the end of the Cold War, which changed the focus, operations, modalities and mandates in a big way. The post-Cold War era introduced an information revolution that challenges intelligence sources and methods (Rathmell, 2002:87). The pace of change has left the intelligence organisations out in the cold and has resulted in a crisis management style of dealing with issues. According to Rathmell (2002:88), there is an urgent need to understand the new reality and how to successfully manage it. Postmodernism attempts to provide such a framework that recognises, accommodates and understands global changes within intelligence studies. Rathmell (2002:95–96) identifies five core postmodern themes that he applies to understand the changes within intelligence. These themes are the following:

- The end of grand narratives: The “grand narrative” came to an end with the end of the Cold War. Postmodernism substituted the “grand narrative” for fragmented worldviews with no unified theories of the social world or knowledge.
- The end of the search for absolute truths: Postmodernism does not subscribe to “objective truths” and recognises the role of the researcher as an “agent or participant”.

- Absent centres and uncertain identities: According to postmodernism, technological, social and economic changes are breaking down individual identity boundaries, leaving a society with an uncertain identity.
- Fluid boundaries: Postmodernists believe social change, technological developments and economic progress caused blurred boundaries among states, regions and corporations, creating an environment that ignores sovereignty of states.
- The knowledge economy: Technological development and specifically the communication technology have given rise to the knowledge economy. (Rathmell, 2002:95–96).

With these themes as introduction, Rathmell (2002:97–98) goes further and applies them to intelligence in the following manner:

- Fragmentation of targets and roles: Whereas modernity focused and underlined "linearity" in developments, postmodernity focuses on "non-linearity and chaos". This can be illustrated by the end of the Cold War. During the Cold War, events were incremental and "linear" and this gave intelligence services an identifiable framework to operate within. However, after the end of the Cold War intelligence services had to deal with unknown developments that were not part of the known framework, they seemed "non-linear" and chaotic. Within the new chaotic narrative, the intelligence community must deal with new targets and carve out a new role. Intelligence studies cannot continue to work in the Cold War framework.
- Mysteries not puzzles: During the Cold War intelligence communities had certainty with regard to their role, function and targets. However, the end of the Cold War has diminished the certainty and intelligence communities are faced with a reality they do not know or understand.
- Identity: During the Cold War intelligence communities knew exactly who the targets were and who the clients of their products were. Since the end of the Cold War and as a result of technological development, information has been available to all members of society not only restricted to intelligence communities. Intelligence communities are faced with uncertainty with regard to targets and clients.
- Fluid boundaries: During the Cold War clear boundaries existed within which the intelligence community performed their tasks. However, after the end of the Cold War, these boundaries became fluid and the cooperation between the private sector and intelligence has increased a great deal. Cooper (2002:2) indicates that some of the characteristics of the postmodern state are the "growing irrelevance of borders" and that

security is “based on transparency, mutual openness, interdependence and mutual vulnerability”.

- The end of the intelligence factory: Technological developments are changing the way intelligence organisations are doing business, specifically with regard to the collection process.

With this detailed discussion of postmodernism in intelligence as background, it is also important to mention additional postmodern characteristics relevant to this study. Other characteristics of postmodernism in relation to intelligence include the following:

- This approach uses Sherman Kent’s (1966:ix) definition and views “intelligence as a kind of knowledge” and the main business of intelligence is the production of “targeted, actionable and predictive knowledge for specific consumers” (Rathmell, 2010:87–102).
- Postmodernism refers to the rise of new approaches to knowledge and the process of creating knowledge (Rathmell, 2010:87–102).
- Blurred lines between foreign and domestic policy (Cooper, 2002:2).
- Security is based on transparency, mutual openness, interdependence and mutual vulnerability (Cooper, 2002:2).
- Rejection of force in the resolving of disputes (Cooper, 2002:2).

Rathmell’s (2002:97–98) arguments correspond with the previous discussion on the current global security situation where it was reasoned that a new way of looking at the security environment is needed. Within the study of intelligence, realism has always been the main approach. However, some aspects of realism are no longer applicable, especially since the end of the Cold War. The end of the Cold War together with the communication technology developments has opened up the global playing field, allowing for other role players than states to influence global political developments. States are no longer the only role players within the international political arena; non-state actors actually pose a greater threat to security than state actors. Although it is still a new approach, this study suggests that postmodernism does offer an alternative to the understanding of intelligence in the post-Cold War information era, especially as it recognises that we are working in a new world order where boundaries are blurred and the state is not the only element in the international political system. The approach of postmodernism in intelligence provides a better framework to understand this study and especially SOCMINT. This is particularly true if one takes into account that one of the most important developments within the media environment is the replacement of the traditional broadcast media by interactive personalised media (social

media). This underlines the importance of a framework for this significant untapped source of information within the intelligence community. Postmodernism provides the best theoretical basis for this study in understanding the phenomenon of social media and its implications and applications within the intelligence environment.

The three conceptual frameworks have been clarified in the previous section. This provides the grounding for the final element of the conceptual framework of social science research, namely concept and definition. The next section explains the concept and definition of intelligence.

3.4 Concept and definition of intelligence

As mentioned in Chapter 2, the most basic component of scientific research is concepts. In this respect, the most basic concept within the field of intelligence studies is intelligence. Currently there is no agreement on the definition for the term intelligence. According to Warner (2002:15), there is an urgent need for an agreed definition to theorise and fully understand intelligence. He furthermore highlights the fact that each author uses his/her own definition without building or referring to each other (Warner, 2002:15). Even though there is not an agreed term, most definitions do refer to or use Sherman Kent's (1966:ix) definition of intelligence as "the knowledge which our highly placed civilian and military men must have to safeguard the national welfare". In addition, Kent (1966:ix) mentions the three "distinct things" or dimensions intelligence practitioners refer to when they use the word intelligence: knowledge, organisation and activity. These dimensions can be summarised as follows:

- Intelligence as an activity or process (Kent, 1966:ix): These activities include collection, evaluation, analysis, integration, interpretation and dissemination. The process of intelligence is also referred to as the intelligence cycle (Figure 16). For example: The information related to the expected terror attack is obtained by means of intelligence.
- Intelligence as a product (Kent, 1966:ix): The product is defined as the end result of the intelligence activity. For example: The intelligence regarding the terror attack will be provided to the Minister.
- Intelligence as an organisation (Kent, 1966:ix): The intelligence organisation is the unit engaging in the process and production of intelligence. For example: Intelligence will be tasked with obtaining the relevant information regarding the terror attack.

While most authors refer to Kent's (1966:ix) definition of intelligence, they highlight their own version or interpretation. Gill and Phythian (2006:1) explains that a worthwhile definition of intelligence should include the full range of activities of intelligence agencies and the purpose supporting these activities. They furthermore indicate that security is the end result of intelligence (Gill & Phythian, 2006:1). They define intelligence as "an umbrella term referring to the range of activities (from targeting through the information gathering to analysis and dissemination) that are conducted in secret and aimed at maintaining or enhancing security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventative policy or strategy" (Gill & Phythian, 2006:1).

Unlike Gill and Phythian (2006:1), Warner (2002:15) succinctly describes intelligence as "secret, state activity to understand or influence foreign entities". Even though the definition is succinct, it indicates a range of activities in which intelligence communities are involved. These "state" activities include the intelligence process of collection, analysis, CI and covert action. All these activities are focused on understanding foreign role players, where foreign role players include any foreign government and non-state actors posing a threat to the national security of the country. The influence portion of the definition also includes the use of covert action. Countries can influence other parties or other countries through the use of covert action (detailed discussion in Chapter 4). While Gill and Phythian (2006:1) and Warner (2002:15) refer to intelligence as "secret state activities", Sims (1995:4) only refers to "information" in his definition of "information collected, organised or analysed on behalf of actors or decision makers". This definition is too broad as it indicates all information. With regard to intelligence, the important aspect or element is secret information and it should be built into any definition of intelligence (Shulsky, 1995:17). While previous definitions are succinct, Lowenthal (2006:9) has a more convoluted definition that includes all the aspects to which Kent (1966:ix) refers. According to this definition, intelligence "is the process by which specific types of information important to national security are requested, collected, analysed and provided to policy makers; the product of that process; the safeguarding of these processes and this information by counterintelligence carrying out of operations as requested by lawful authorities" (Lowenthal, 2006:9).

Whereas most definitions use Kent's (1966:ix) proposal as basis, Breakspear (2013:692) is proposing a "new definition for intelligence" with a focus on its forecasting possibilities. He proposes the following definition: "Intelligence is a corporate capability to forecast change in time to do something about it. The capability involves foresight and insight, and is intended to identify impending change, which may be positive, representing opportunity, or negative,

representing threat" (Breakspear, 2013:692). According to him, this definition facilitates a better understanding of intelligence and enables better oversight and evaluation of intelligence (Breakspear, 2013:692). This proposed focus on forecasting is of great importance in the current global environment of new threats and continuous technological developments.

In the South African context, the White Paper on Intelligence (1995) guides the policy framework within which the intelligence services should function. The White Paper (South Africa, 1995:2) defines intelligence as "the product resulting from the collection, evaluation, analysis, integration and interpretation of all available information, supportive of the policy and decision-making processes pertaining to the national goals of stability, security and development". Modern intelligence can be described as "organised policy related information, including secret information" (South Africa, 1995:2). The intelligence can be gathered overtly or covertly from various sources, including human, non-human, open and secret sources. According to the White Paper (South Africa, 1995:2), intelligence has to be accurate, relevant and timely and have a predictive capacity and an element of early warning to be of value to the policy maker. The White Paper (South Africa, 1995:2) definition focuses, just as Lowenthal (2006:9), on all the aspects of Kent's (1966:ix) definition.

For the purposes of this study, intelligence is defined as follows:

- the collection of information pertaining to all threats and opportunities from all available sources;
- the analysis, integration and interpretation of information into a product; and
- the timeous dissemination of the final product to the national client to assist in policy decisions.

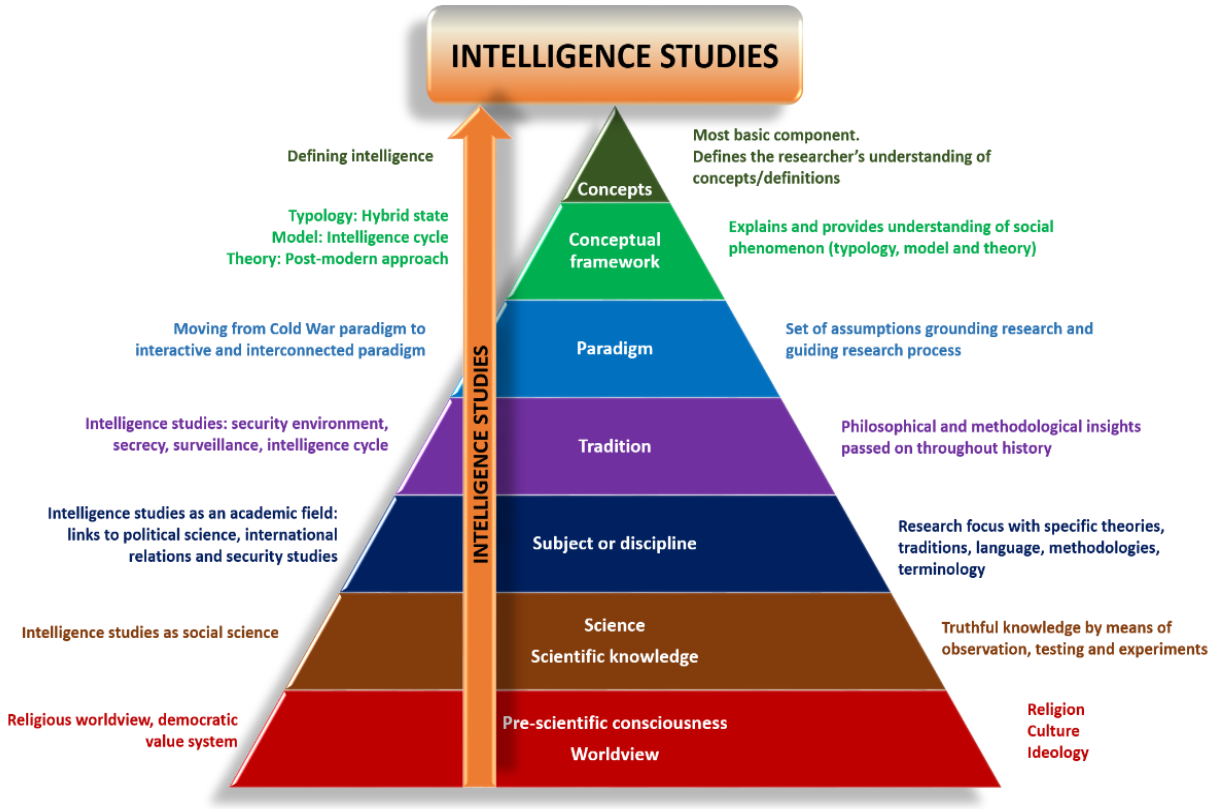
All these activities take place within the secret environment of the intelligence organisation and is guided by the priorities and feedback provided by the national client. It is important to include all available sources as this leaves room for the inclusion of information from social media. Furthermore, the inclusion of all threats accommodates the CI environment (see Chapter 5).

This discussion of the concept of intelligence concludes the framework for social science research as referred to at the start of this chapter. The next section brings together the discussions of Chapter 2 and 3 into a framework for the understanding of the intelligence

component of SOCMINT. Chapter 4 provides more detail on the new media component of SOCMINT.

3.5 Conceptual framework for understanding intelligence within this study

As mentioned on various occasions and illustrated in Chapter 2, this study is a combination of two academic fields, intelligence studies and new media studies. This study has as objective the construction of a framework to understand and incorporate SOCMINT into the national security environment. In order to successfully reach this objective, there is a need to ground this study in respect of theory in general and metatheory in particular. Previous discussions have laid the basis for such a metatheoretical framework. This conceptualisation is depicted in Figure 21 and consists of the important metatheoretical departure points for this study as it relates to intelligence studies.



Source: Adapted from Duvenhage, 1994:60; Greffrath, 2015:29

Figure 21: Conceptualisation of intelligence

The conceptual framework for the understanding of social science research is used as a basis to explain the intelligence component of SOCMINT and is depicted in Figure 21. The discussions started in Chapter 2 with the development of a seven-element framework of

social science research. The first element of social science research is the pre-scientific consciousness or worldview. This study is grounded in a religious worldview and politically based in a democratic value system. With regard to the second element, science and scientific knowledge, this study belongs to the social sciences, in particular the political science discipline. Intelligence studies resorts under the sub-discipline of security studies, which is a sub-discipline of international relations under political science. The next component is tradition and for the purposes of this study, the security environment, secrecy, surveillance and the intelligence cycle are viewed as intelligence traditions. The fifth element is paradigms and it was explained why this study subscribes to an interactive and interconnected paradigm. The next element is conceptual frameworks, which includes typology, models and theory. For the purposes of this study the hybrid state, the intelligence cycle and the postmodern approach were discussed. The final element of the framework is the concept and in this regard, an intelligence definition was proposed. All these elements comprise a framework for the intelligence component of SOCMINT.

3.6 Conclusion

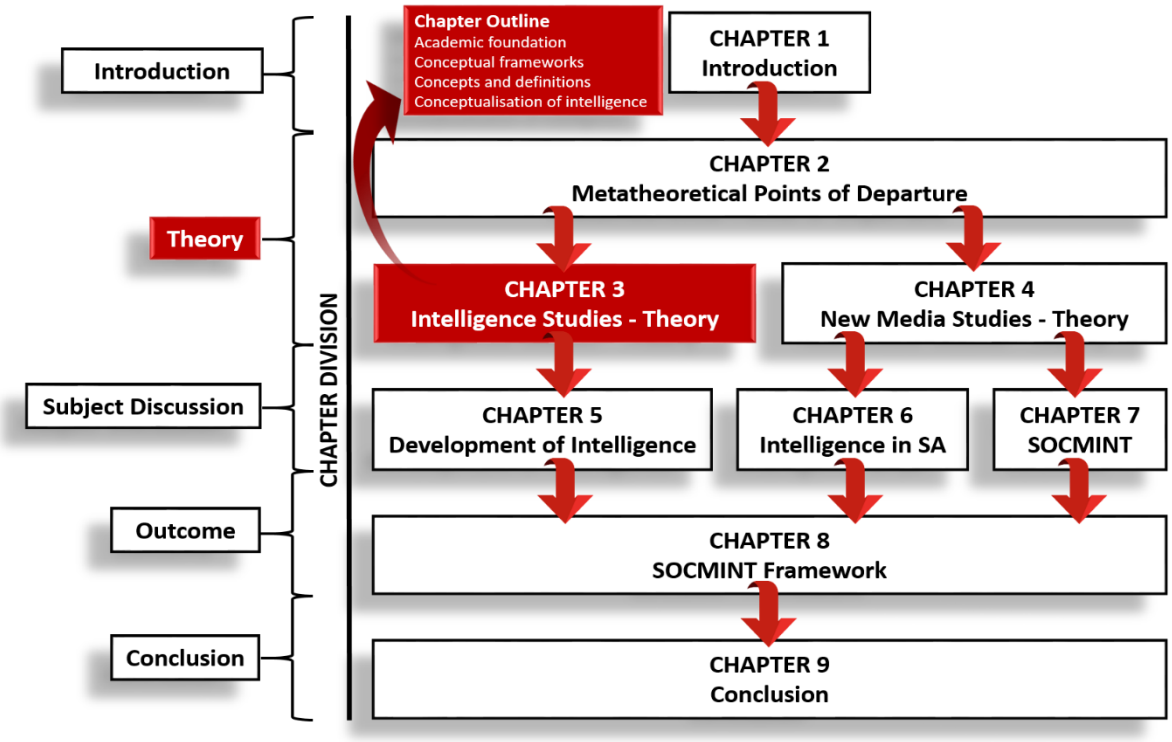
In order to contribute to the body of scientific knowledge it is important to theoretically ground a study. This chapter had as its principle objective the conceptualisation of intelligence. This was done along the lines of the social science research framework compiled in Chapter 2.

As suggested before, the theoretical base of intelligence studies is limited. This study is a contribution to that theoretical base. In order to reach the main objective, the following secondary objectives were also addressed:

- Understanding the academic links to intelligence studies, including political science, international relations and security studies.
- Explaining the current state of intelligence studies as an academic discipline, taking into account that it is still a young field.
- Understanding and elaborating on the conceptual frameworks that is dominant in intelligence studies.
- Clarifying the concept of intelligence to understand the academic field.

The main outcome of this chapter is a conceptual framework to understand intelligence studies. In order to reach this outcome, the chapter started with a detailed discussion on the

origins and academic links of intelligence studies to the fields of political science, international relations and security studies. This was followed by a discussion of intelligence studies as an academic field and the reasons why it is currently not viewed as a discipline. As tradition and paradigm were discussed in Chapter 2, the following section continued to discuss the various conceptual frameworks. These included typology, models and theories. With regard to theories it was argued that with the current global context in mind, postmodernism is the best approach for the study. Finally, the concept of intelligence was discussed as the last element of social research. Defining intelligence remains a contentious issue and various definitions were highlighted before an appropriate definition for this study was compiled. The chapter concluded with the conceptualisation of the intelligence component of SOCMINT. The main outline of this chapter and its position within the study is depicted in Figure 22 below.



Source: Own construct

Figure 22: Chapter 3 Summary

The next chapter focuses on the metatheoretical departure points for new media and on metatheory, theory and conceptual orientations. This concludes the theoretical base for this study.

CHAPTER 4: NEW MEDIA STUDIES – METATHEORETICAL, THEORETICAL AND CONCEPTUAL ORIENTATION

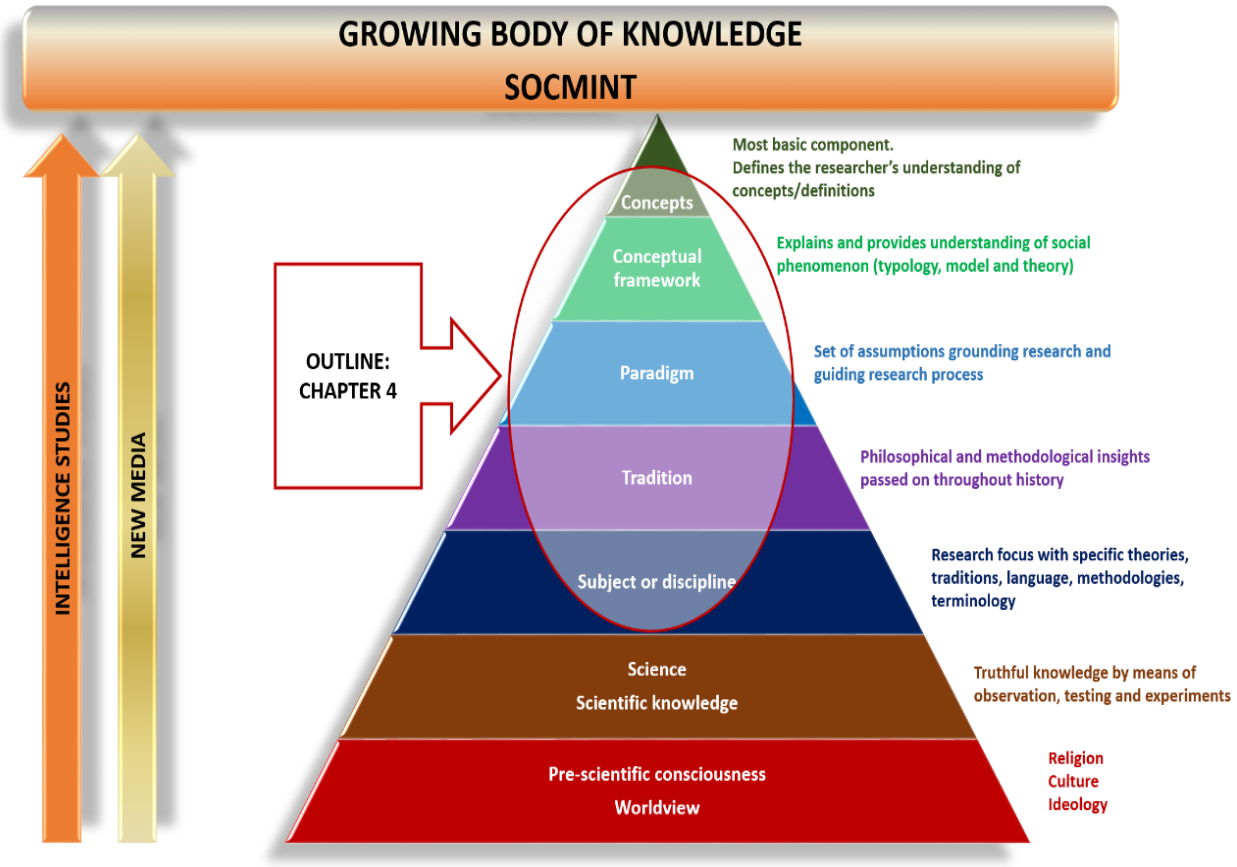
"Social media is changing the way we communicate and the way we are perceived, both positively and negatively. Every time you post a photo, or update your status, you are contributing to your own digital footprint and personal brand."
Amy Jo Brand (brainyquote.com)

4.1 Introduction

As explained in Chapter 2, a metatheoretical framework is of great importance to guide the research process. Chapter 2 presented a conceptual framework to understand SOCMINT in terms of the metatheory and the combination of intelligence and new media studies. This conceptual framework was applied to the intelligence studies component of this thesis in Chapter 3. The theoretical base of this study is rounded off in this chapter with the development of the metatheoretical and theoretical base of the new media studies component.

The main focus of this chapter is therefore to conceptualise social media along the lines of the framework developed in Chapter 2 (Figure 23). The main areas of discussion are the following:

- The chapter begins by discussing the academic foundation of social media.
- The next section focuses on traditions within the field of new media studies. Chapter 2 highlighted this issue in passing, and it is discussed in greater detail here.
- This section is followed by the paradigm within the new media field that is relevant to this study.
- The chapter then turns to conceptual frameworks within new media studies, with specific reference to typology, models and theories.
- The next part clarifies some important concepts, such as hypertext and social media sites.
- This is followed by a conceptual framework for new media studies as the final element of SOCMINT.
- The chapter concludes with a conceptual framework for SOCMINT, combining intelligence studies (Chapter 3) and new media studies (current chapter).



Source: Adapted from Duvenhage 1994:60; Greffrath, 2015:29

Figure 23: Outline: Chapter 4

The discussions is based on the metatheoretical framework for the understanding of social sciences as developed in Chapter 2. This framework identifies seven components for social science research: pre-scientific consciousness or worldview, science and scientific knowledge, subject or discipline, tradition, paradigm, conceptual framework and concepts. These elements are discussed in relation to new media studies. Pre-scientific consciousness for this study refers to the religious worldview and was discussed in detail in Chapter 2 (see Section 2.4.1). This particular worldview is relevant to this study and is also applicable to this section of new media studies. With regard to the second component of social science research, science and scientific knowledge, Section 2.4.2 highlighted that media studies belongs to the social sciences, as is the case with intelligence studies.

The field of SOCMINT is a new field of interest and there is a shortage of publications on the field, especially in relation to theoretical perspectives and inputs. Omand *et al.*[25] have written various publications on SOCMINT and could be regarded as the leaders in the field. However, the focus of their research is more on the SOCMINT content and not on the theory surrounding the subject. This study attempts to address the theoretical basis of SOCMINT. The first section of this chapter focuses on the discipline of communication sciences and how it relates to the field of new media studies.

4.2 Subject or discipline

New media studies belongs to the discipline of communication science and resorts under the field of media studies. It is necessary to give a brief overview of communication science to understand the origins of new media studies.

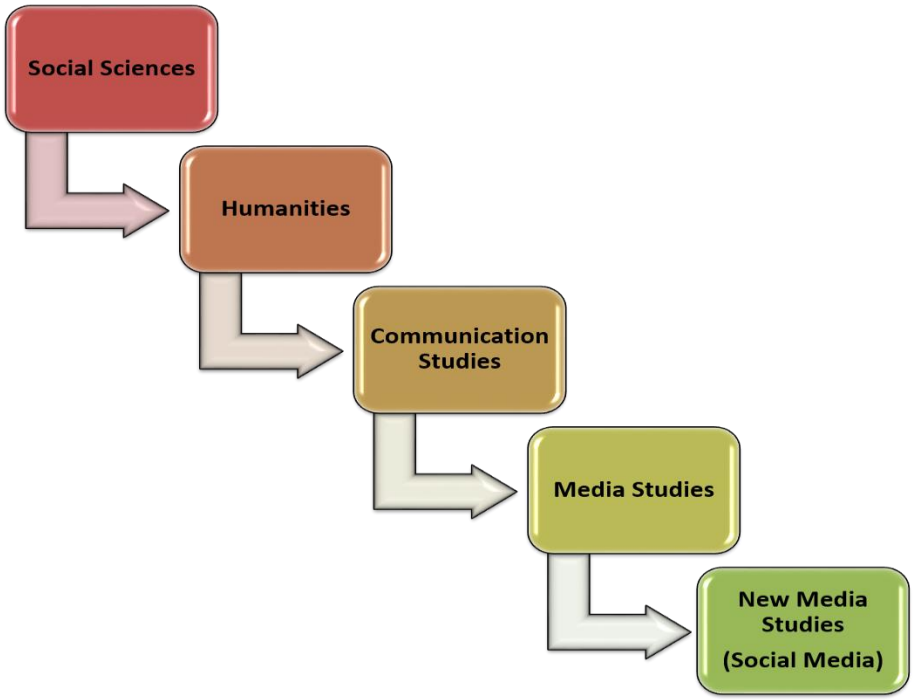
Even though the concept of communication has been with us for a long time, the discipline of communication science is a relatively new academic field (Craig, 2009:959; Simonson & Peters, 2008:765). The formalisation of the study of communication only started during the late 19th century and during this time the main discipline was political economy with sociology as the sub-field (Simonson & Peters, 2008:765). The early academic focus of this field was on newspaper studies: history, statistics and the organisation of the press system (Simonson & Peters, 2008:765). The first institute devoted to science of the press (Institut für Zeitungswissenschaft) was founded in 1916 by Karl Bücher at the University of Leipzig (Simonson & Peters, 2008:765). The focus of communication studies moved to propaganda during World War I and the Russian revolution (Simonson & Peters, 2008:765). The inter-war period focused on film and radio. By the mid-1940s the field was known as "communication research" (Simonson & Peters, 2008:766). The inter-war period also saw the start of mass communication research, especially in light of the radio technology (Simonson & Peters, 2008:766). World War II provided the opportunity for international collaboration on issues related to communication. During the post-War period various views came from different regions. As part of its foreign policy of propagating democracy and the belief that the press is an important role player in democracy, the United States of America established schools of journalism in Japan (Simonson & Peters, 2008:768). While it was part

[25] See Omand, D. 2013. Social media: the security challenge; Omand *et al*. 2012. Introducing social media intelligence (SOCMINT); Omand *et al*. 2012. #Intelligence, and Omand *et al*. 2014. Towards the discipline of social media intelligence.

of its foreign policy objectives to spread democracy, it is suspected that these actions were also intended to increase its influence in the Asian region.

During the beginning of the 1960s, communication studies was still part of departments such as sociology, psychology and political science. However, since 1968 communication and media studies were viewed as a discipline and became centralised in independent schools or departments of communication (Parcell, 2008:757; Simonson & Peters, 2008:768).

New media theory is a very young field within media studies. According to Holmes (2009:684), this field was only formalised in the 1990s. There is constant debate on what new media is, for old media was previously new media. The current focus of new media is ICT and specifically the interactive nature of the technology (Parcell, 2008:763). New media has in recent times come to refer to media in relation to digital or electronic media and therefore some scholars refer to it as the "digital media", "interactive communication", "digital communication", "hyper media", "networked or collaborative communication" (Lister *et al*., 2003:12; Scolari, 2009:945–946).



Source: Own construct

Figure 24: Academic links of social media

This study views new media studies as part of media studies within the discipline of communication sciences. New media studies is part of media studies, which is part of

communication studies, which resorts under humanities and social sciences. These academic links of new media is depicted in Figure 24. The digital or new media of today has changed the media landscape on various levels. It is true especially in relation to information production, distribution and access. With regard to production, the ICTs have opened up this previously restricted area to everybody with access to a computer or smartphone and the internet. The content can then be available to everybody with a computer, phone and internet across the globe. Digital media is always present and has stimulated an opinionated society.

With this clarification of new media studies' disciplinary roots, the next step is to explore the theoretical character of this field. The next section focuses on traditions within the field of communication sciences.

4.3 Tradition

As indicated in Chapter 2 (see Section 2.4.4), every academic discipline has beliefs, practices and principles that are transferred to the next generation. This is also relevant to communication studies. This section first focuses on traditions within the communication discipline. This discussion is followed by contexts of communication to improve our understanding of the communication process.

Craig (1999:119–132) argues that communication is not a coherent field and lacks principles of a universal theory. In an attempt to find common ground, Craig (1999:135–149; 2009:960–962) has identified seven traditions that each focuses on a different aspect of the field, divided according to "underlying conceptions of communicative practices". These traditions are depicted in Figure 25 below.

Source: Adapted from Craig, 1999:135–149; West & Turner, 2010:28

Figure 25: Traditions of Communication theory

Craig (1999: 135–149; 2009:960–962) explains these traditions as follows:

- Rhetoric: According to the Concise Oxford English Dictionary (2004:1233), rhetoric is defined as "the art of effective or persuasive speaking or writing". Rhetoric is the oldest tradition and has its origins in ancient Greece and Rome where debate was practised extensively in the city-state environment. This is a powerful tool of communication, especially in relation to influencing and formulating opinion. Craig (1999:135) describes it as "a practical art of discourse". For this reason it is viewed as a significant tradition of communication theory. The rhetoric tradition can also be applied to the study of social media. Information on social media can be used to influence people and encourage new opinions. The use of social media can be illustrated by referring to the events of the Arab Spring during which social media was used to influence political change in countries such as Tunisia and Egypt (Howard *et al*., 2011:8; Liaropoulos, 2013:9; Safranek, 2012:5).
- Semiotics: This is also known as the study of signs and refers to a process of using signs to convey messages.
- Phenomenology: This tradition conceptualises "communication as the experience of self and other in dialogue" (Craig, 2009:960). According to Orbe (2009:749), this approach "focuses on the conscious experience of phenomena contextualised within the world

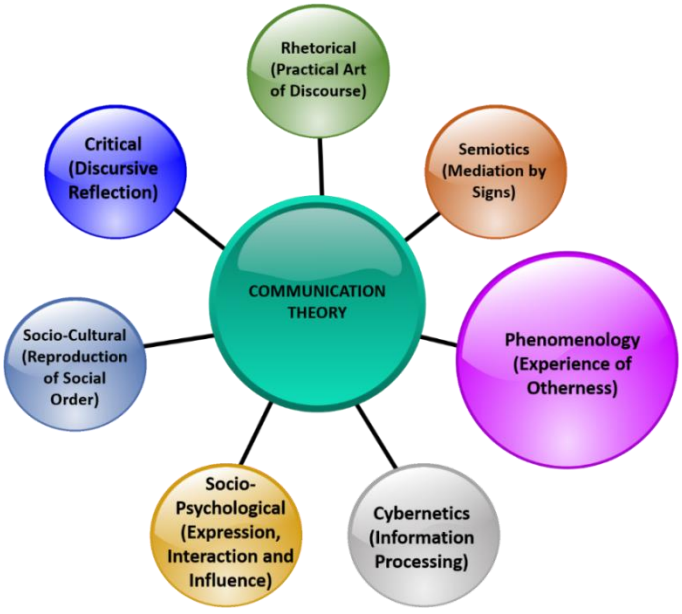
individuals inhabit" and "phenomenology is the study of essence, or the person's lived experience in his or her life world before it gets categorised and theorised". Within the tradition of phenomenology, knowledge is gained from experiences to which we assign meaning and meaning is determined by the importance of that particular phenomenon (Van Rheede van Oudtshoorn, 2011:21). The knowledge gained from the experience is then explained by using language (Van Rheede van Oudtshoorn, 2011:21). For the purposes of this study, phenomenology can be described as personal experience and the experiences of others as communicated through language (written and spoken); in the case of this study, also through social media. This study focuses on the phenomenon of social media, and phenomenology is the study of how people experience social media. The analysis of social media produces SOCMINT.

- Cybernetics: Wiener (1961:11) defines cybernetics as the "field of control and communication" applicable to "machine or in animal". Kolmogorov (cited by Novikov, 2016:11) has a more convoluted definition and describes cybernetics as "a science concerned with the study of systems of any nature which are capable of receiving, storing and processing information so as to use it for control". In addition, Van Rheede van Oudtshoorn (2011:49) explains that the simple objective of cybernetics is to understand the function and processes of systems. This tradition grew from theories in electrical engineering and it conceptualises communication as information processing. An important element of cybernetics is feedback. Krippendorf (2008:1153) explains that feedback is essential for learning. The element of feedback is also underlined by Dubberly and Pangaro (2010:3), as they define cybernetics as a "discipline for understanding how actions may lead to achieving goals. Knowing whether you have reached your goal requires feedback". This tradition can also be applied to this study of social media and SOCMINT in particular. In order to understand how cybernetics can be applied to SOCMINT, Kolmogorov's (cited by Novikov, 2016:11) definition and Van Rheede van Oudtshoorn's (2011:49) explanation of the objective of cybernetics are relevant. The aim of intelligence is to understand processes and systems that influence national security. Social media enables the creation of systems such as networks (terrorism networks) that could have negative implications for national security. Intelligence organisations analyse these networks to produce actionable intelligence.
- Social psychology: According to this tradition, communication is conceptualised as a social interaction and influence. Communication always takes place between two or more people. Each person brings with them their specific personality characteristics, attitudes and emotions. There is influence in this communication environment, which is also relevant in the larger context of mass media. This tradition can be applied to the field of social media. People's social behaviour is the basis for this tradition and the focus

is on communication between two or more individuals and the influence they have on each other. Social media is a communication medium between individuals or a group of individuals. The phenomenon of social media has brought with it a new dimension to the social psychology tradition. People no longer need to meet face to face; they can communicate with users all over the globe without leaving the comfort of their home. This medium of communication is also powerful with regard to influencing and mobilising people, which is evident from various events around the globe (see Chapter 7).

- Sociocultural theory: This tradition is derived from sociological and anthropological thought and conceptualises communication as a process of interaction that produces and reproduces shared meanings, rituals and social structures (Craig, 1999:144). The tradition of sociocultural theory can also be applied to this study. Social media provides users the opportunity to communicate on issues of common interest, share opinions and create an online community (see Chapter 6 for characteristics of social media).
- Critical theory: According to this theory communication is conceptualised as discursive reflection or discourse in which the implicit assumptions behind what was said can be questioned and discussed to achieve mutual understanding (Craig, 1999:146).

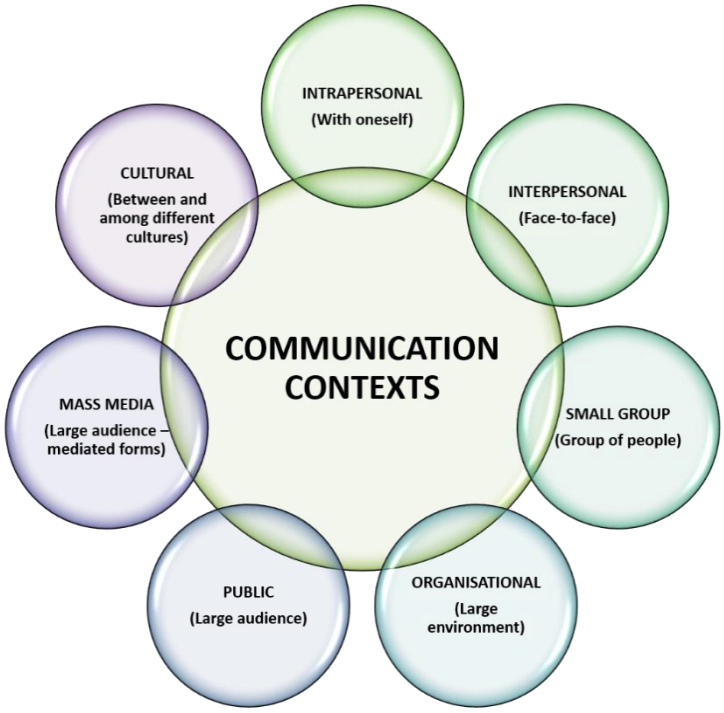
From the discussions above it is clear that the tradition relevant to this study is phenomenology (Figure 26). This relates to research objective 6 as set out in Chapter 1: Studying the social media phenomenon and identifying the threats and opportunities to national security and how these can be applied within the intelligence environment. Studying the phenomenon of social media enables us to reach this objective.



Source: Adapted from Craig, 1999:135–149; West & Turner, 2010:28

Figure 26: Phenomenology Tradition relevant to this study

It is also important to discuss the context of communication to create a more practical framework for understanding communication theory and the traditions in particular (West & Turner, 2010:32). The main focus of the West and Turner (2010:32) framework is context, which refers to the "environments where communication takes place". These contexts or environments give the researchers the background to analyse the communication phenomenon (West & Turner, 2010:32). This framework is portrayed in Figure 27 below.



Source: Adapted from West & Turner, 2010:33

Figure 27: Contexts of Communication

While Craig (1999:119–132) is of the opinion that communication lacks the principles of a universal theory, West and Turner (2010:32) argue that there seems to be universal agreement on the contexts of communication. To support their argument they mention that most communication departments at academic institutions are formed along the lines of the seven contexts as depicted in Figure 27 above (West & Turner, 2010:32).

The first context described by West and Turner (2010:32) is that of intrapersonal communication or communication with oneself. This type of communication allows a person to acknowledge their own abilities and it takes place intentionally or unintentionally (West & Turner, 2010:32–34). For example, am I an excellent worker? The focus of research in this context is on cognition, symbols and intentions of individuals (West & Turner, 2010:34). While it is expected that this type of communication takes place when reading online social

media posts and news feeds (debating internally the truth of the posts or news), it is not relevant to this study.

Interpersonal communication is the second context and is also referred to as face-to-face communication (West & Turner, 2010:34). The focus of this context is on relationships according to West and Turner (2010:34), "rich with research and theories" because of its complexity and diversity. This context can also be applied to the social media environment. One of the most important characteristics of social media is its interactivity (Boyd & Ellison, 2008:211; Montagnese, 2012:5–6; Omede, 2015:275; Safranek, 2012:2; Schein *et al*., 2010:4). These characteristics are discussed in greater detail in Chapter 7. While the interactivity of social media does not imply physical face-to-face communication, it can be viewed as part of interpersonal communication. The latest communication technologies have opened up a new type of communication that allows immediate and face-to-face communication through applications such as Facetime and Skype.

Another context is small group communication, which is composed of a number of people working towards a common goal (West & Turner, 2010:35). According to West and Turner (2010:35), a small group is communication between at least three people. The size of the group has specific implications for relationships and goals. The bigger the group, the more personal relationships and the greater the possibility of not reaching the goal (West & Turner, 2010:35). The small group communication context is less relevant to social media. While social media groups might start out small, the global nature of social media means that they usually end up large. The basic aim of social media is to reach as many people as possible in the shortest possible time. This context is therefore not relevant to this study.

The fourth context is that of organisational communication, usually organisations where hierarchy plays an important role (West & Turner, 2010:37). According to West and Turner (2010:37), theories in this context are typically focused on how the organisation operates. This context is also not relevant to the social media environment, as hierarchy does not play a role within the social media communication structure. While a movement on social media (for example #FeesMustFall) is usually created or started by a particular person, the movement gets a life of its own and anybody can join and post comments. Leadership does not play a role and nobody reports to anybody.

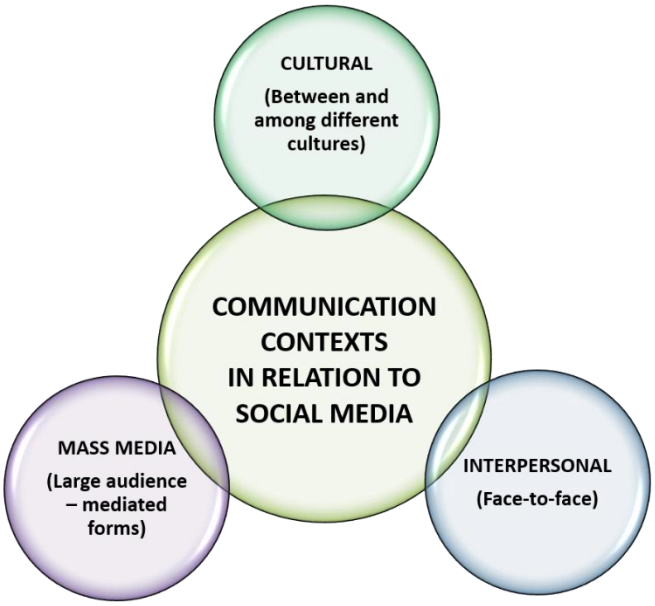
The next context West and Turner (2010:38) identify is the public or rhetorical communication context. This is the context of public speaking and is characterised by the distribution of information from one person to a large group (West & Turner, 2010:38). The

research associated with this context is communication apprehension, or the fear of public speaking. This context is not relevant to social media. Although social media does involve communicating to a big group, it is usually anonymous and not public speaking as much as it is public writing.

Mass or media communication is the sixth context and focuses on large audiences (West & Turner, 2010:40). In this context mass media is the way in which news is distributed (TV, radio, newspaper and internet) and mass communication is the communication to a large audience through the mass media (West & Turner, 2010:40). The context includes both mass communication and mass media. The focus of research in this context is wide-ranging and usually relates to the impact of mass media or mass communication on the audience (West & Turner, 2010:40). This context is highly relevant to new media and to this study. In this regard and for the purposes of this study, this context includes mass communication through social media platforms to a large audience (globally) with access to computers and internet.

The final context West and Turner (2010:41) discuss is that of cultural communication. West and Turner (2010:41) describe culture as “communication between and among individuals whose cultural backgrounds vary”. This context is also relevant to the study of social media. Communication through social media takes place across cultures and across country boundaries.

Although it is important to highlight the various contexts within the communication field, it is equally crucial to indicate the contexts that are relevant to this study. From these discussions the interpersonal, cultural and mass or media contexts are applicable to social media and therefore to this study. These contexts are depicted in Figure 28 below.



Source: Adapted from West & Turner, 2010:33

Figure 28: Contexts of Communication – relevant to this study

The changes in the technology environment and the impact on social interaction have brought about new traditions that were discussed in the section above. In the same manner new technologies, especially the internet, have changed traditional media paradigms that guided the understanding of the previous analogue mass-media environment. The discussion below explains paradigms within the communication sciences that are applicable to the new global situation.

4.4 Paradigm

Digital technology has fundamentally changed the communication and specifically the media landscape. It has changed the relations with the audience (currently more interactive); it has created new languages (multimedia), new grammar (hypertext) and new role players (anybody with a phone and internet access) (Kaul, 2012:6; Orihuela, 2003:1). Orihuela (2003:1) coins this new environment the “eCommunication”, which is a shift from traditional media to the digital media. Various authors have raised the issue of paradigm change in communication (Kaul, 2012:1; McQuail, 2013:216; Mora, 2012:139). According to McQuail (2013:218), “it has hardly been in question that public communication is well on the way to being better represented by a new paradigm, although no single name has been coined”. He

is also of the opinion that the features of the new paradigm reverse some of the "fundamental pillars of the old one" (McQuail, 2013:218).

McQuail (2013:218) and Kaul (2012:1–9) highlight the following as the primary characteristics of communication according to the new paradigm:

- Digital technology provides interactivity, allowing the user to control what and how they view content.
- There is open and ready accessibility to channels to send and receive information. This implies that information can be transmitted anytime and anywhere.
- Digital media allows for the use of multimedia, such as photos, text and videos.
- There is a lack of central control and regulation of supply and choice.
- Digital media offers unlimited capacity with regard to access to content.
- There are low or negligible transmission costs.
- There is no fixed location. Content is distributed globally, from anywhere in the world.
- There is diversity and flux of control, content and uses. The users can decide themselves what to watch and when to watch it.

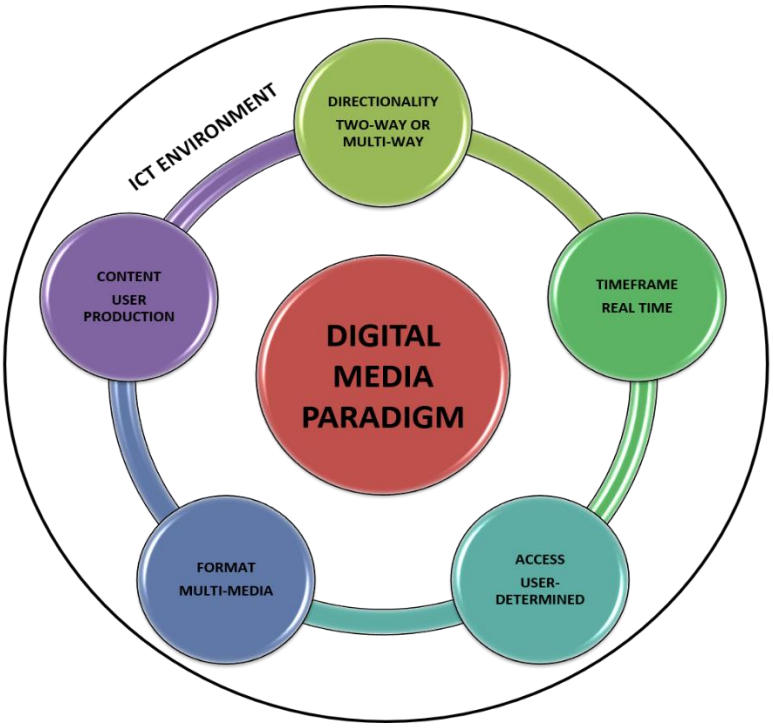
These characteristics match up with the typology of old and new media that is discussed in section 4.5.1.

For the purposes of this study the new communication paradigm is called the digital paradigm. This paradigm has the following elements:

- Directionality (two-way flow): Traditional mass communication (TV and newspapers) has always been one-directional (Neuman, 2008:2319). However, with new media such as social media, consumers are no longer just receivers of information, they actively participate by uploading information and interacting with information online (Neuman, 2008:2319; Orihuela, 2003:4).
- Time frame (real or synchronic time): Information is distributed immediately and is available as soon as it has been distributed (McQuail, 2013:218; Orihuela, 2003:3).
- Access (user-determined): Users have the choice of accessing information or data whenever they want and for as long as they want (McQuail, 2013:218; Neuman, 2008:2319; Orihuela, 2003:3).

- Content (user-driven): People are no longer observers or passive recipients of media content, but are also participants in that they can create and comment on content (Orihuela, 2003:3).
- Format (multimedia): Digital media has enabled the production of content on a single media (online media) where all types of media formats can be arranged together and used interactively (text, photo, video, graphics and animation) (Orihuela, 2003:3).

This new paragraph can be presented as in Figure 29 below.



Source: Own construct

Figure 29: New digital paradigm

This section highlighted the digital media paradigm. This forms the basis for the next segment, which discusses various conceptual frameworks within the field of communication sciences pertinent to this study.

4.5 Conceptual framework

The conceptual frameworks have been explained in great detail in Chapter 2 (see Section 2.4.6). This section only refers to conceptual frameworks as they relate to communication sciences, in particular new media. These frameworks include typologies, models and theories.

4.5.1 Typology

One of the principle typologies within the media studies framework is old and new media. Traditional media is defined as “the non-electronic medium which is a part of our culture and is used for transmitting tradition from one generation to another” (Newme, 2011:56). The Collins Online Dictionary describes it along the same lines as “media before the arrival of the internet, such as newspapers, books, television and cinema”. New media (also known as digital media) on the other hand, is defined as “content created, disseminated, and stored using digital computers or mobile devices” (Chun, 2008:1314). For the purposes of this study, this definition is applied.

This study relates to new media, it is therefore important to highlight the differences between old and new media. The table below clarifies these differences.

Table 4: Typology of new media

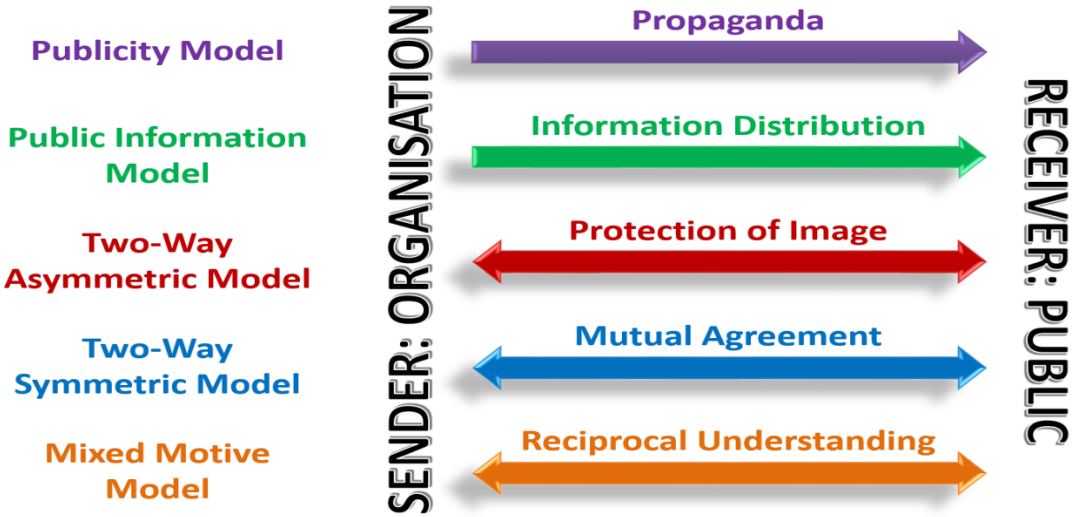
TYPOLOGY CRITERIA	OLD MEDIA	NEW MEDIA
Format or means of communication	Radio – Sound TV – Audio-visual Newspapers – paper	Digital – cell phones, laptops, tablets and computers.
Communication direction	One-way communication	Two-way, interactive communication. Can provide opinions and comments instantly.
Networking	No networking – one-way communication	Networking as a result of two-way communication options.
Production of content	Media companies, journalists, publishing companies	User-generated content. Anybody with access to internet and cell phones, laptops, tablets and computers.
Environment	Reality	Virtual.
Scope and reach	Limited by country boundaries Country-specific	Global - only limited by internet access.
Audience	Consumer	“Prosumer”- consumer and producer of content.
Content access	In total and when available	Articles of interest, by means of hypertext, when convenient to the user.

Source: Ahuja, 2015; Salaverria, 2017:20; Lister *et al*., 2003:13; Ruggiero, 2000:15

This segment focused on typology of new and old media as the first conceptual framework. The next section examines models within communication sciences, which is the second conceptual framework.

4.5.2 Models

As mentioned on various occasions, social media has changed the media landscape and therefore models are needed to understand this phenomenon. However, before the model relevant to this study is discussed, it is necessary to first highlight various communication models (Figure 30).



Source: Adapted from Marin, 2007:49–50

Figure 30: Communication models

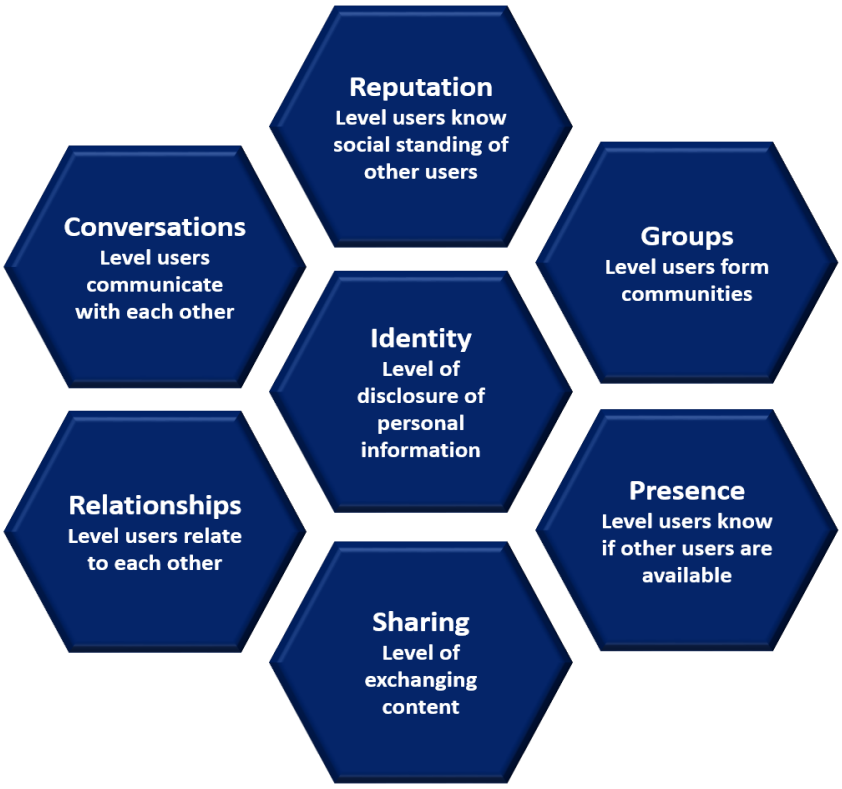
The first is the press agentry/publicity model (Dozier *et al*., 1995:41; Grunig & Hunt, 1984:22). This model is characterised by a one-directional flow of information from the organisation to the public and the main purpose of the information is publicity, so truth is not essential (Dozier *et al*., 1995:41; Marin, 2007:49). The next model is the public information model (Dozier *et al*., 1995:41; Grunig & Hunt, 1984:22). This is one-way flow of truthful information about the organisation, transmitted from the organisation to the public (Marin, 2007:49). The third model that Grunig and Hunt (1984:22) identify is the two-way asymmetrical model. The model is characterised by a two-way flow of information, the organisation communicates to the public and any feedback from the public is used to the advantage of the organisation (Dozier *et al*., 1995:41; Marin, 2007:49). The next model is the two-way symmetrical model (Dozier *et al*., 1995:41; Grunig & Hunt, 1984:22). This model is similar to the previous, with the difference that feedback from the public is used to the

advantage of both the public and the organisation (Dozier *et al*., 1995:41; Marin, 2007:49). The final model is the mixed-motive model that was developed as a result of views that the two-way symmetrical model was too idealistic (Wiggill, 2009:36). The characteristic of this model is reciprocity or mutual benefits, where organisations understand that by conceding to some demands from the public, they also benefit (Wiggill, 2009:36).

While not all the models discussed above can be applied to social media, the mixed-motive model can be applied to this study. Social media can be viewed as two-way, reciprocal communication, where both the sending users and receiving users are equally advantaged. However, it is important to also discuss a model that is specifically relevant to social media. The "honeycomb of social media" model is suitable in this case (Kietzmann *et al.*, 2011:243–248). Kietzmann *et al*. (2011:243–248) developed this model to understand the functional building blocks of social media. This model was developed to assist companies with establishing strategies for monitoring, understanding and responding to different social media activities (Kietzmann *et al*., 2011:249).

The model consists of seven blocks (Figure 31), all constructing a honeycomb. It is discussed in terms of its functionality and implication:

- Identity: This block indicates the level to which users reveal their identity on the social media sites. Most social media sites require users to provide their personal information in setting up their profiles on that specific site. This information is available to that company, but can also be mined as in the case of Facebook®.
- Conversation: Most social media sites are created to facilitate conversation between likeminded users.
- Sharing: The sharing of information includes the distribution and receiving of information.
- Presence: This provides knowledge of users' availability and their location.
- Relationships: This block indicates how users are related or connected.
- Reputation: This block refers to trust of that particular user. This block is more relevant to businesses as they a need good reputation for their business.
- Groups: This block relates to the degree to which users can form groups or communities (Kietzmann *et al*., 2011:243–248).



Source: Adapted from Kietzmann *et al*., 2011:243

Figure 31: Functional building blocks of social media

While Kietzmann *et al*. (2011:243) developed this model for the purposes of business firms, it can also be applied to the intelligence framework and to this study.

The model as applied to the intelligence environment can be explained as follows:

- Identity: Intelligence organisations can use users' personal information on social media websites during investigations.
- Groups: The information contained in the group can be utilised by the intelligence community to determine relationships, interests and plans.
- Presence: From an intelligence perspective, one can create a profile of, for instance, the movements and availability of a specific person.
- Sharing: This information can assist intelligence organisations to compile a profile of the interests of a particular user. This information can be used to establish contact and to determine the person's relations with other users.
- Relationships: This information provides intelligence on relations, networks, affiliation and contacts. This information is crucial, especially in counter-terrorism cases.

- Conversations: Conversations that take place on social media sites create networks. The information pertaining to the networks and the conversations themselves are of great importance to intelligence organisations. This information can assist intelligence organisations to profile people, conversation topics, links to other users and to identify and establish contact with a potential source.
- Reputation: Social media is the electronic form of word-of-mouth. This information can give an indication of the mood of the people in terms of how prominent people or organisations are viewed.

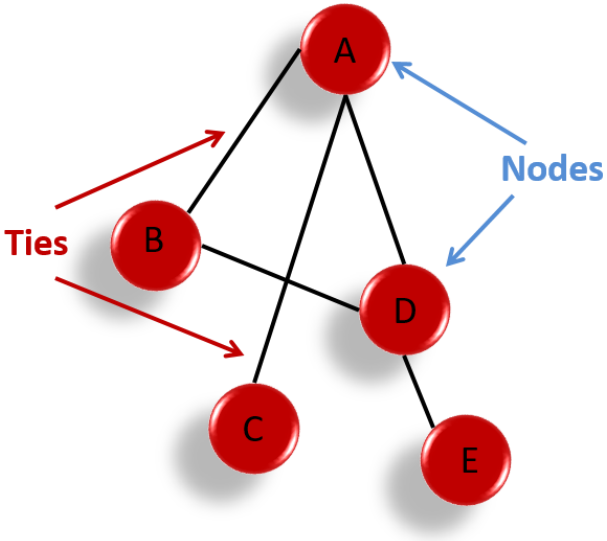
The third and final conceptual framework, theories, is discussed in the next section.

4.5.3 Theory

Social media has changed various aspects of our daily lives, ranging from the way we conduct business to the way we socially interact. This new phenomenon also has implications for the research and academic environments. Ngai *et al*. (2015:33) conducted a study to ascertain the extent of research with regard to theories, constructs and conceptual frameworks in the field of social media. The group analysed 46 articles on social media and identified three groups of theories: personal behaviour, social behaviour and mass communication (Ngai *et al*., 2015:35). Two theories are relevant to this study of SOCMINT. These theories include social network analysis and the uses and gratification theory. Another issue that is of importance to this study is interactivity. While this theme is not on the list compiled by Ngai *et al*. (2015:33), the theory of interactivity is also discussed. Although there are more theories that could be applied to SOCMINT, this study does not allow for an elaborate discussion of all applicable theories. For a detailed list see Ngai *et al*. (2015:35).

The first theory is social network theory. This theory helps to explain how relationships within networks work. According to Halgin (2012:3), social network theory is increasingly being applied to social media websites. In its most basic form a network is “a set of relationships that contains a set of objects (nodes) and a mapping or description of relations between the nodes” (Halgin, 2012:3; Kadushin, 2012:13). In this regard and for the purposes of this study, social network theory is the study of the relationships within a network. According to Scott (2000:7), modern social network theory only came about in the 1960s and has been shaped by three traditions of research: the socio-metric tradition (in relation to graph theory), interpersonal relations tradition (in relation to cliques) and anthropology tradition (structure of community relations).

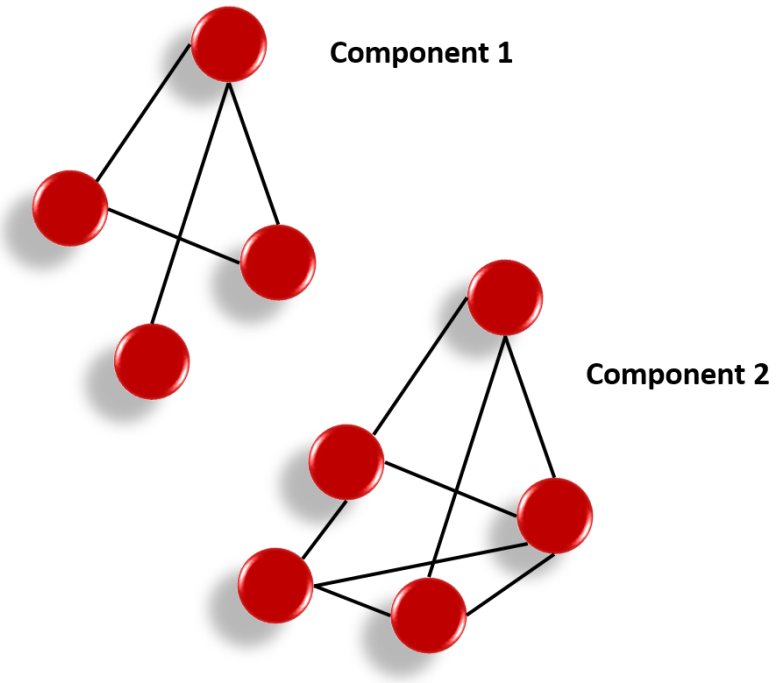
A network consists of two elements: nodes and ties (Borgatti & Halgin, 2011:2; Halgin, 2012:3), which are depicted in the figure below. Nodes are individuals or a cluster of individuals (organisation), while ties are the links between the nodes (Borgatti & Halgin, 2011:2; Halgin, 2012:3).



Source: Adapted from Halgin, 2012:5

Figure 32: Elements of a network

Nodes can either be directly or indirectly linked to each other. In Figure 32 above, A and B and A and D are directly linked, while A and E are indirectly linked via D. The patterns created by interconnected nodes form a particular structure and within that structure, nodes occupy positions (Borgatti & Halgin, 2011:2; Halgin, 2012:3). Furthermore, a network consists of components. In Figure 33 below, the network consists of two components, 1 and 2.



Source: Adapted Borgatti & Halgin, 2011:2

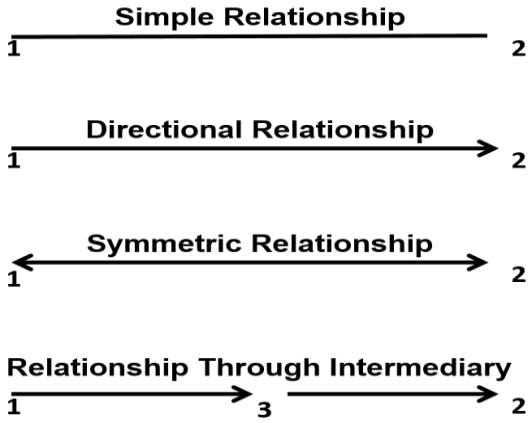
Figure 33: Network with two components

According to Borgatti and Halgin (2011:2), there is a distinct difference between a group and a network. The difference lies in the boundaries. A group has particular boundaries, while a network does not have natural boundaries (Borgatti & Halgin, 2011:2). This is particularly relevant to social media, in that social media networks are formed across the globe and do not adhere to physical borders and boundaries. Additionally, ties can be divided into two categories: relational states and relational events (Borgatti & Halgin, 2011:3; Halgin, 2012:6).

Borgatti and Halgin (2011:3) describe the categories as follows:

- State-type ties:
    - Kinship ties such as a sister or father.
    - Role-based ties such as manager.
    - Cognitive – knows.
    - Affective – likes.
- Relational events:
    - Interaction – giving advice.
    - Transactions – making a sale.

While the communication tradition did not initially contribute to social network theory, the development of ICT has given rise to a new collaboration between media effect research within the field of communication and social network theory (Liu *et al*., 2017:2). Kadushin (2012:13) argues that social network theory can be applied to groups of various sizes: small groups, organisations and international systems. These relationships can vary from simple relationships, directional relationships to symmetric relationships and relationships through an intermediary (Kadushin, 2012:14–15). These relationships are depicted in Figure 34 below.



Source: Adapted from Kadushin, 2012:14–15

Figure 34: Network relationships

Network theory is especially relevant to this study. It is especially in the case of terrorist organisations and social unrest that networks and the analysis of networks can play a crucial role in obtaining intelligence. It is important to ascertain the relationship between members of a group and their links to other groups or people. With this analysis one can determine the most important person or persons within a group and resources can be focused on that particular person to obtain intelligence.

The second theory relevant to this study is the uses and gratification theory. This theory is one of the theories of mass media and is concerned with why consumers use a certain medium of communication. This theory deals with questions such as: Why do people use a specific type of mediated communication, and what gratification do they receive from it (McQuail, 2010:352; Ruggiero, 2000:29). The use of a specific media format depends on satisfaction, needs, wishes or motives of the users (McQuail, 2010:352). Katz *et al*. (1974:510) are of the view that people use or pursue a specific type of media and specific content to create a specific gratification. Originally these research projects mainly focused on

reasons why people use mass media (Sherry & Boyan, 2008:5239), but the theory is also applicable to new media studies. According to Sherry and Boyan (2008:5239), uses and gratification theory is one of the oldest and largest continuous programmes of research within the communication discipline. The development of new communication technology has resuscitated the uses and gratification theory (Quan-Haase & Young, 2010:351; Ruggiero, 2000:3). The reason is that the new technologies have increased consumers' choices and it is important to understand the motivation and satisfaction gained from using a certain media source to analyse the pattern of media use. This theory can also be applied to social media to explain why social media is used and with what consequences.

When looking at the theoretical base of uses and gratification approach, Katz *et al*. (1974:510–511) highlight five basic assumptions:

- The audience is active and the media use is goal-oriented. With regard to new media, users are active through new ICTs (internet, computers and mobile devices), commenting and raising their opinions on social media websites. Furthermore, users use different social media sites for different reasons. These sites include profile-based social media sites (organised around the users' profile pages) such as Facebook® and content-based social media sites (the user's profile is used to organise connections) such as Flickr (photos) (SAS, 2012:2; Abdulhamid *et al*., 2011:15–16).
- The initiative to link need gratification to a specific medium choice rests with the audience member. In relation to new media, users have the option to use whatever internet site they want, depending on what requirement they need to fulfil.
- Media compete with other sources for need satisfaction. Different social media sites compete with each other with respect to user preferences.
- People have enough self-awareness of their media use, interests and motives to be able to provide researchers with an accurate picture of that use. As mentioned above, social media users apply different sites for different reasons, depending on their needs.
- Value judgement of media content can only be assessed by the audience.

With this discussion as background, it is important to discuss the application of this theory in relation to social media. Various studies have been done to determine why people use social media by applying the uses and gratification theory (Al-Menayes, 2015:45–48; Froget *et al*., 2013:137; Quan-Haase & Young, 2010:355; Whiting & Williams, 2013:366–367). These studies identify various uses and gratifications for using social media:

- Social interaction: Social media is used to socially interact with friends or likeminded people.
- Information-seeking: Social media can assist with finding information on products or businesses.
- Pass time: Social media is used to pass time.
- Entertainment: Social media can also be a form of entertainment to play games, listen to music and watch videos.
- Relaxation: Social media is used to relax and take the user's mind off other issues.
- Communicatory utility: Social media provides topics for discussion.
- Convenience utility: Social media is accessible at any time and in any place.
- Expression of opinion: Social media is used to comment and express opinions on issues at hand.
- Information sharing: Social media is used to share personal information.
- Surveillance or knowledge about others: Social media is used to keep track of acquaintances. (Al-Menayes, 2015:45–48; Froget *et al.*, 2013:137; Quan-Haase & Young, 2010:355–356; Whiting & Williams, 2013:366–367).

These uses and gratifications are explored in greater detail in the discussion of SOCMINT in Chapter 7.

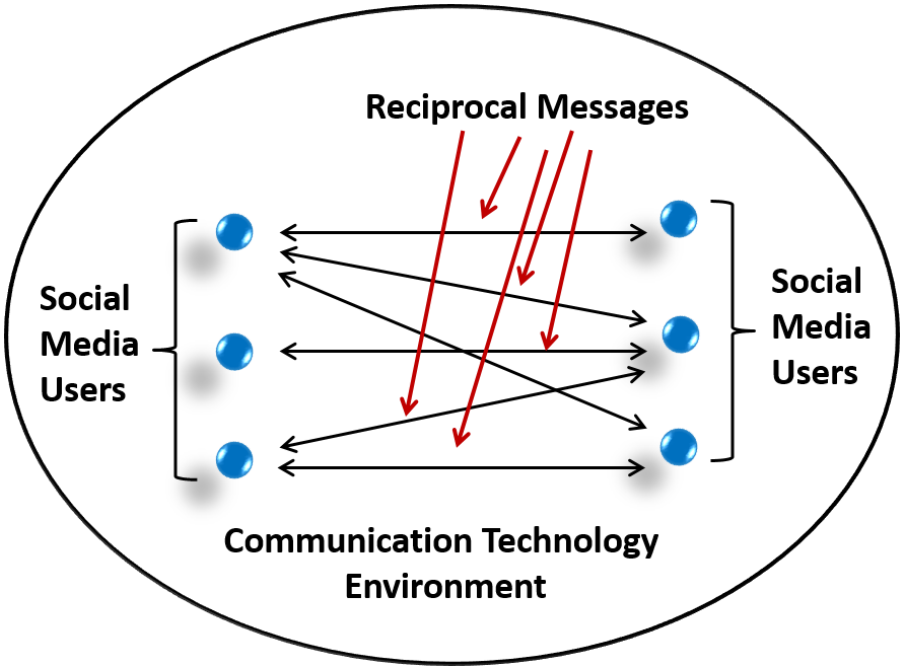
The final theory is the theory of interactivity. Interactivity is associated with new communication technology (Kiousis, 2002:356; Neuman, 2008:2318). One of the characteristics of new media is its interactivity, which is a feature of all new communication technologies. It is therefore imperative that paradigms within communication sciences, particularly new media studies, also include interactivity. While it is necessary to define the concept of interactivity, it is important to mention that there is no single definition of this term (Ariel & Avidar, 2015:21; Jensen, 1998:185; Kiousis, 2002:357). Definitions of interactivity include proposals from the communication and non-communication disciplines (Kiousis, 2002:363). However, for the purposes of this study, the focus is on definitions related to the communication discipline. Rafaeli (1988:110–111) describes it as an "under-defined concept" and defines it as "an expression of the extent that in a given series of communication exchanges, any third (or later) transmission (or message) is related to the degree to which previous exchanges referred to even earlier transmissions". From this definition an important characteristic of interactivity can be identified, namely third order dependency. Third order dependency implies that messages respond to and implicate previous messages (Kiousis, 2002:359). According to Williams *et al*. (1988:10), "the degree

to which participants in a communication process have control over, and can exchange roles in their mutual discourse is called interactivity". Kiousis (2002:372) researched various definitions and he defines interactivity as "the degree to which a communication technology can create a mediated environment in which participants can communicate (one-to-one, one-to-many and many-to-many), both synchronously and asynchronously, and participate in reciprocal message exchange". For the purposes of this study, the definition of Kiousis (2002:372) is used.

From the definition of interactivity, Kiousis (2002:368) identifies the following elements that are of importance when *operationalising* the definition of interactivity:

- It is a two-way or multi-way communication
- Usually through a mediated channel
- The roles of message sender and receiver are interchangeable
- Communication can be in human or machine form
- Individuals are able to manipulate the content
- Different levels of interaction exist

From the discussion above the definition is applied to social media in Figure 35 below. Social media enables two-way or multi-way communication by means of communication technology such as the internet, computer and mobile devices; messages are reciprocal (sender and receiver are advantaged by the communication); and, users can manipulate the content.



Source: Own construct

Figure 35: Interactivity of social media

This section highlighted the sixth component of the social science research framework, namely conceptual frameworks. It is also important to unpack concepts within the field of new media as the final component.

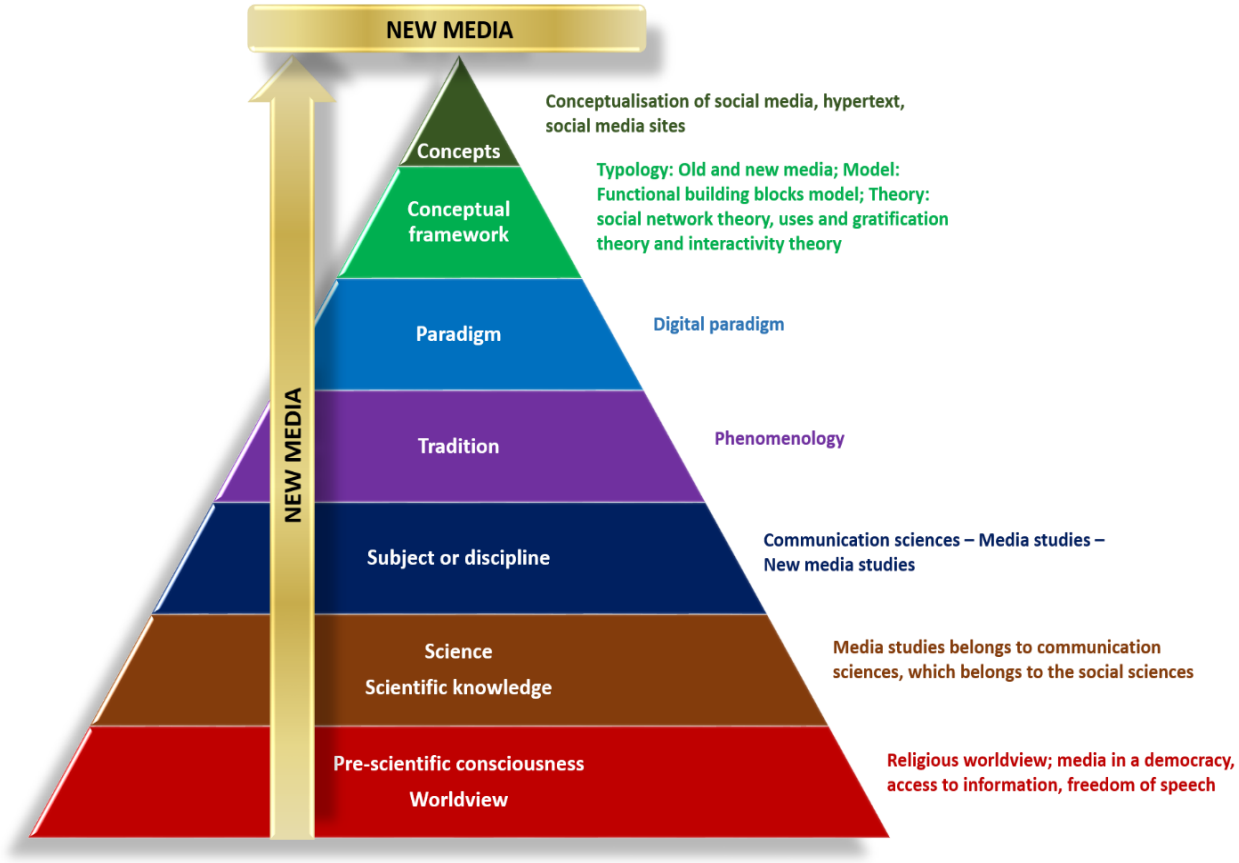
4.6 Concepts and definitions

The final component of the social science framework is concepts. The concept of social media is explained in detail in Chapter 7. However, various other concepts should also be clarified. One of the concepts that are used often within the field of digital environment is hypertext. According to Lister *et al*. (2003:26), hypertext is "a text which provides a network of links to other text that are outside, above and beyond itself" and "a work which is made up from discrete units of material, each of which carries a number of pathways to other units". The structure of hypertext allows users to seek further information of interest (Lister *et al*., 2003:26). Another concept that needs clarification is social media sites or platforms. These sites are web-based sites that allow users to construct a profile that is public or semi-public, list the users they share the connection with, create user-generated content and have a conversation with those within the system/list (Abdulhamid *et al*., 2011:14; Boyd & Ellison, 2008:211; Brunty *et al.*, 2013:1).

With this discussion of metatheoretical departure points in new media studies as background the next section focuses on a conceptual framework to understand new media within this study. This complements the framework for intelligence studies compiled in Chapter 3.

4.7 Conceptual framework for new media studies

The conceptual framework for the understanding of social sciences as developed in Chapter 2 (Figure 10) is used as a basis for conceptualising new media studies. This framework highlights seven elements of social science research. These elements are applied to new media studies below (Figure 36).



Source: Adapted from Duvenhage 1994:60; Greffrath, 2015:29

Figure 36: Conceptual framework for understanding social science research in reference to New Media Studies

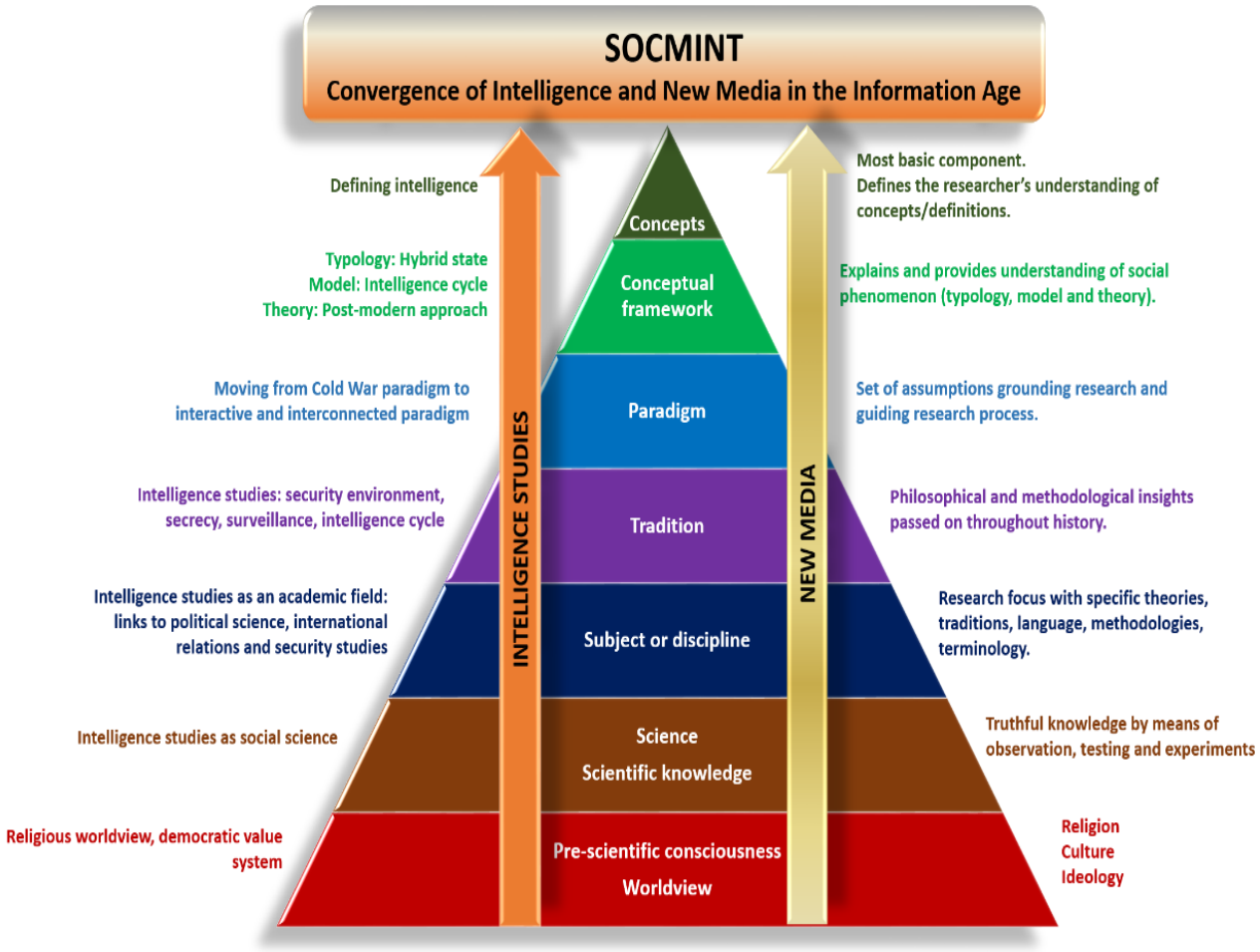
With regard to the first element, this study is based on a religious worldview with a democratic government system of free access to information and freedom of speech. The second element of this framework is science and scientific knowledge. This study is grounded in the social sciences. In relation to the third element, subject or discipline, new

media studies belong to media studies within the discipline of communication sciences. The next component is tradition and in this regard phenomenology was highlighted as the preferred tradition. The paradigm that is relevant to this field of study is the digital media paradigm. The next component is conceptual frameworks, which includes typologies, models and theory. For the purposes of new media studies, the typology of new and old media, the functional building blocks model and social networks, uses and gratification and the interactivity theories are relevant. The final element of this framework is concepts. The concepts of hypertext and social media sites are explained. All these elements together provide a metatheoretical framework for the new media component of SOCMINT (Figure 35).

The chapter concludes with a conceptual framework for SOCMINT that incorporates both the conceptual frameworks from intelligence studies and new media studies.

4.8 Conclusion

The main aim of this study is to develop a strategic framework that incorporates the new phenomenon of SOCMINT into the intelligence environment. As explained and illustrated in Chapter 2, this study is a combination of intelligence studies and new media studies. It was demonstrated in Chapter 2 that to reach the objective it is important to ground this study in a metatheoretical framework. Chapter 3 provided the metatheoretical framework to understand intelligence studies. The discussion in this chapter provides the background for a conceptual framework for new media studies, which is depicted in Figure 36. From these deliberations in Chapter 3 and 4, a metatheoretical conceptual framework for this study can be compiled (Figure 37).



Source: Adapted from Duvenhage 1994:60; Greffrath, 2015:29

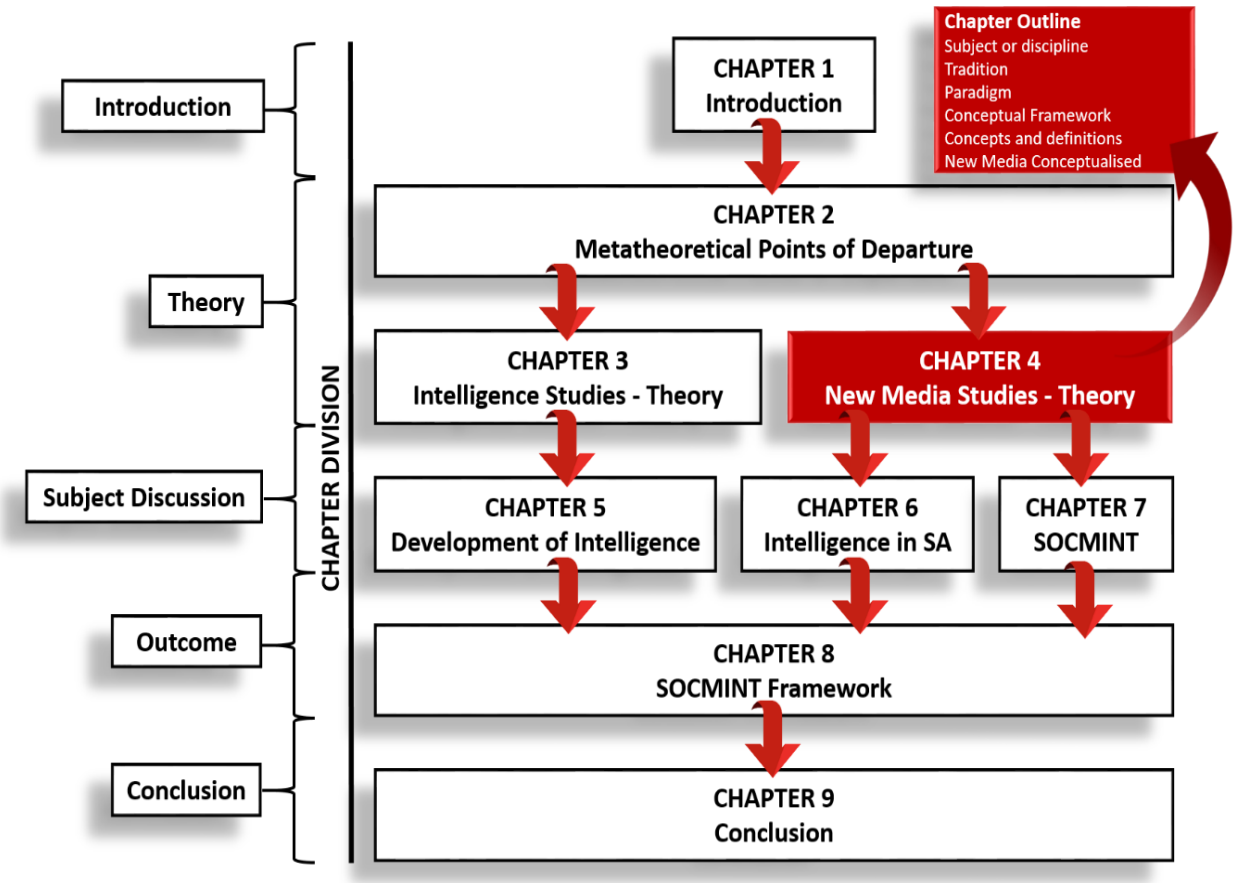
Figure 37: Meta-theoretical conceptual framework for understanding SOCMINT

The following is a summary of this metatheoretical framework:

- Pre-scientific consciousness or worldview: The basis for this study is a religious worldview with a democratic value system that embraces freedom of speech and access to information.
- Science and scientific knowledge: Both intelligence studies and new media studies belong to the social sciences.
- Subject or discipline: Intelligence studies belongs to the discipline of political science under international relations and security studies. New media studies on the other hand, is a sub-field of communication sciences.
- Traditions: Within intelligence studies the main traditions include the security environment, secrecy, surveillance and the intelligence cycle. For the purposes of this study, the phenomenology tradition is applicable to new media studies.

- Paradigm: As a result of the new communication technology it was explained that the interactive and interconnected paradigm is the best suited for the current global environment. This is closely linked to digital paradigm relevant to new media studies.
- Conceptual frameworks: Three conceptual frameworks were identified for the purposes of this study: typology, models and theories. With regard to intelligence studies, the relevant typology is that of a hybrid state, the intelligence cycle model, and the postmodernism theory. New media applies the old and new media typology; the functional building blocks model; and social network, uses and gratification and interactivity theories.
- Concepts: The concepts of intelligence, social media sites and hypertext were explained.

This conceptual framework provides the theoretical base for SOCMINT that is discussed in great detail in Chapter 7.



Source: Own construct

Figure 38: Chapter 4 Summary

The summary of this chapter and how it relates to other chapters in this study is depicted in Figure 38. The main aim of this chapter was to conceptualise a metatheoretical framework for new media studies. The chapter started with a discussion on the academic foundation of new media studies. This was followed by the unpacking of traditions, paradigms, conceptual frameworks and concepts relevant to new media studies. The chapter concluded with a metatheoretical conceptual framework for SOCMINT, which includes intelligence studies and new media studies.

This chapter concludes the theoretical base for this study (Chapter 1, 2, 3 and 4) and provides the foundation for the following chapters. The next chapter outlines the evolution and development of intelligence and how it links up with the development of technology. As this study of SOCMINT is a culmination of intelligence and technology, it is important to find the common ground between the two areas of interest and establish how intelligence was influenced by the development of technology.

CHAPTER 5: THE EVOLUTION OF THE INTELLIGENCE PROFESSION AND THE ROLE OF TECHNOLOGY

Technology was a key driver in the intelligence revolution of the Twentieth Century.
Wesley K. Wark (2003)

5.1 Introduction

Chapter 4 focused on the academic foundation, theories, concepts and definitions of new media studies. This discussion culminated in a conceptual framework for the understanding of new media studies. The chapter concluded with a conceptual framework for the understanding of SOCMINT.

Against this background, it is important to examine the history of the intelligence profession to supplement our understanding of this field. Matey (2005:15) highlights that we have to study the past to define intelligence. Theodore Roosevelt commented that "the more you know about the past, the better prepared you are for the future". Even though intelligence is a young field, it is important to study its history to learn and prepare for the future.

This chapter provides the historic background of intelligence by clarifying its evolution from espionage. However, as explained previously, this study with its focus on SOCMINT is a combination of intelligence studies and new media studies. SOCMINT is a product of ICT development. It is imperative to also investigate technological development and its impact on the development of intelligence to pursue the research objective of this study, which is to *investigate intelligence and social media to develop a strategic framework that incorporates the new phenomenon of SOCMINT into the intelligence environment, explaining its role within the intelligence cycle, its application as a source of information and the threats and opportunities related to it.*

When examining history it is clear that technology played a crucial role in the development, application and role of intelligence during various events. However, the exact role is difficult to ascertain because of the secret nature of the intelligence profession. Andrew and Dilks (1984:1) refer to intelligence as "the missing dimension" mainly because of the secrecy surrounding intelligence and records that are not easily assessable. The main goal of this chapter is to explain and understand the evolution of intelligence and to clarify the role technology played in this process. In order to fully understand intelligence development it is imperative to recognise the development of technology and how it enhanced the activities of

intelligence organisations throughout history. Furthermore, technology is an important aspect of this study. Social media is one of the recent technological developments that has major implications for the security environment. For this reason, it is also important to understand the history of technology development.

The development of ICT had a huge effect on various aspects of life in general and on intelligence in particular. It is especially ICT development since the end of the Cold War that is of importance to this study, as this is the time when the phenomenon of social media started. Aronson and Cowhey (2015:3) mention three important developments within the ICT environment that had a profound impact on international relations and therefore also on intelligence organisations. These include the expansion in the use of PCs, the growth of the mobile wireless (cell phone industry) and the internet with its commercialisation (Aronson & Cowhey, 2015:3–4). These technologies changed social interaction within society, creating a new dimension of communication within a world of virtual reality that is increasingly seen as the new reality. Castells (2010b:xvii) refers to this new social structure in the information age as the "network society". This new society is communicating, interacting and mobilising in the virtual world of the internet. This creates threats (illegal activities and mobilisation) and opportunities (information available as a result of activities) to national security.

In the study of the evolution of intelligence it is not only important to highlight technology development and its implications, it is also imperative to understand the primary purpose and functions of intelligence. This provides the parameters within which the intelligence community should operate and links closely with technology development, since technology impacts directly on the functions of intelligence, particularly the collection process. Chapter 3 touched on these aspects when the intelligence links to politics were discussed (see Section 3.2.1). However, a more detailed discussion is necessary to explain how technology fits into the development of intelligence.

With this brief background in mind, this chapter first highlights the primary purpose, functions and elements of intelligence. The purpose and functions of intelligence provide the answer to why intelligence is needed, while the elements describe how intelligence is being conducted. The elements include collection, analysis, CI and covert actions. This section is followed by a discussion on the development of intelligence and the role technology played in its development. Important historic events frame this discussion. The next section addresses events that serve as a framework for the discussion of the evolution of intelligence and the impact of technology development during each stage. Even though technology only features from the renaissance period, the discussions begin in the ancient times for the sake of

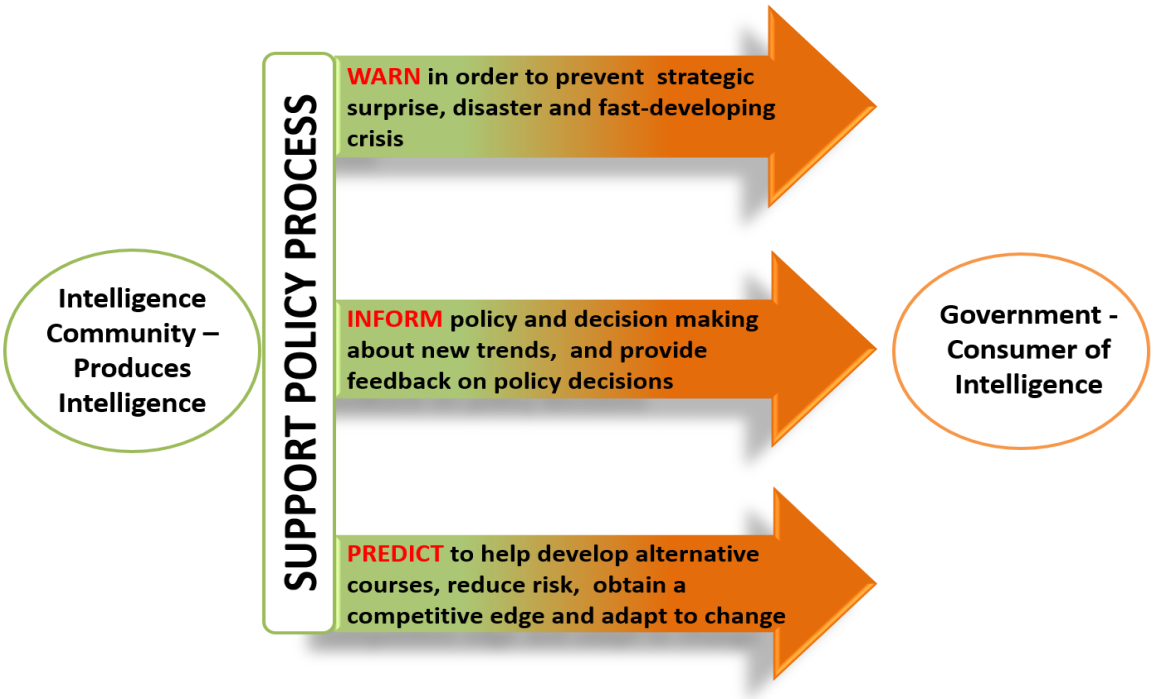
completeness. The chapter concludes with a table illustrating the development of intelligence and the effect of the corresponding technology development during each event on the timeline.

5.2 Purpose and functions of intelligence

Before the development of intelligence can be contextualised, it is important to first understand the purpose and function of intelligence. The main purpose of intelligence has not changed over the ages. The main purpose of intelligence is to support the policy process (Lowenthal, 2006:2–4). It is apt to expand this description to include national security. The purpose of intelligence is to support the policy process for the preservation of national security. According to the Geneva based DCAF (2003:7), policy makers can only make sound decisions if they are sufficiently informed about internal and external security issues. This information is provided by the intelligence community. This also implies that the intelligence community must be aware of the government's policy issues and priorities. According to the intelligence cycle, these policy issues and priorities are defined based on requirements. In the case of South Africa, requirements (national intelligence priorities) are formulated based on the National Intelligence Estimate (NIE). It is important that the intelligence community participate in the formulation of priorities and requirements because of the conflict between what the government wants to know and what it needs to know (Lowenthal, 2006:54; Meyer, 1987:70). It is the responsibility of the intelligence community to inform government about all threats to national security, even if it is not a priority at that stage, while the final responsibility to act on information lies with government.

In order to fulfil its purpose the intelligence organisation has three functions: warn, inform and predict. The first function of intelligence is to provide the government with early warnings on priority issues to prevent surprises (Classen, 2005:83; Lowenthal, 2006:2). Intelligence focuses most of its resources on priority issues as set out by government. These priorities are monitored to identify developments that will have negative implications for the national security of the country. The implications of these developments are communicated to government so that they can respond with policy changes or policy confirmations. The second function is to inform the client on new trends that could have an effect on national security (positive or negative). The intelligence community should be structured in such a way that it is able to identify and report on new trends within the security field. This helps a government to formulate new policy or reformulate existing policy to address the new trend. The final purpose is to make predictions or forecasts about potential threats and opportunities so that the client can respond. It helps the policy maker to adapt to a changed

environment timeously. The discussion above is depicted in Figure 39. The intelligence community produces intelligence products to support the policy process. This support is in the form of warning, informing and predicting. The intelligence products are disseminated to government for action.



Source: Adapted from Classen, 2005

Figure 39: Primary purpose and functions of intelligence

For the purposes of this study, the primary function of intelligence is threefold: to warn the policy maker of threats to and opportunities for national security, to inform the policy maker about new trends that will affect national security, and to make predictions about future threats and opportunities. Intelligence is provided in support of the policy process to protect national security. The current global environment has increased the need for accurate and timeous information underlining the purpose of intelligence organisations. Accurate and timeous intelligence can only be provided if all sources of information are utilised. New sources of information such as SOCMINT also have to be taken into account.

With the purpose and functions of intelligence explained above, the elements of intelligence should be unpacked before the evolution of intelligence and the influence of technology development on intelligence advancement can be discussed. This is important, as the evolution of intelligence and technological developments relates to these elements.

5.3 Elements of intelligence

The elements of intelligence are also referred to as functions of intelligence and comprise collection, analysis, CI and covert action. These elements correlate with the intelligence cycle discussed in Chapter 3 (see Section 3.3.2). The following discussion focuses on each element to outline the importance and application in the intelligence process.

5.3.1 Collection

Even though all the functions are important, collection might be of greater importance since no reliable product can be produced if there is no information. Lowenthal (2006:68) argues that collection is the "bedrock" of intelligence, implying that without it, intelligence will only be "guesswork". DCAF (2003:1) and Lowenthal (2006:69) define collection as the procurement of information through various methods as guided by government requirements. If the intelligence cycle is taken into account, the first step would be requirements received from government. Requirements are dictated by the security picture, nationally and internationally. These requirements are translated into priorities to determine which issues are more pertinent and need more resources. This process translates into a collection plan. Depending on the information needed, different methods of collection could be applied to obtain relevant information. These methods include the following:

- IMINT, also referred to as photo intelligence. It entails the processing and exploiting of images.
- SIGINT, also referred to as communications intelligence (COMINT). It involves the interception of communications between two entities.
- Measurement and signature intelligence (MASINT) involves information about weapons capabilities and industrial activities.
- HUMINT is also referred to as espionage or spying.
- OSINT is information obtained from sources that are overtly available, such as newspapers, journals, books, conferences and government reports (DCAF, 2003:2; Jensen *et al*., 2013:8; Lowenthal, 2006:76-105; Shulsky & Schmitt, 2002:11).

A number of these collection methods are technology-related (IMINT, SIGINT and COMINT). As is explained later in this chapter, intelligence collection through human sources is the oldest method of obtaining information. However, the development of technology has greatly increased the sources of information. The use of HUMINT is being supplemented by a

variety of technical sources. Although this has positive implications for the availability of information, it also implies that intelligence services have to stay informed of new technological developments and acquire these new technologies. These technologies are in most cases very expensive and it is no surprise that less developed intelligence services would remain focused on human sources for their intelligence.

For intelligence to fulfil its functions as set out in the previous section, it is imperative that the intelligence community stay abreast of global developments and their impact on the internal political and security situation. This implies the collection of information to add value and produce intelligence for the client. For the purpose of this study, collection is defined as obtaining information by different means to adhere to requirements as set by the government. Most intelligence organisations refer to three means of collection; technical intelligence (IMINT, SIGINT and MASINT), human source intelligence and OSINT. The collection process has changed over the past decades and it is important for intelligence services to stay up to date with collection methods and potential collection methods. The technological developments over the past century have positively affected intelligence collection methods. However, there is currently no reference to SOCMINT, which is intelligence collected from social media. As indicated in Chapter 1, social media offers information that can be used by intelligence (see Chapter 7). There is an urgent need to include this intelligence in the intelligence cycle in general and in collection in particular. The aim of this study is to incorporate this new form of intelligence into the intelligence framework to institutionalise its use and application.

While collection is viewed as the foundation of intelligence, analysis produces the very important result of the intelligence process. As stated above, without collection there will be no information. In the same way, without analysis there will be no intelligence product. It is necessary to discuss analysis as the second element of intelligence.

5.3.2 Analysis

Analysis is the process of transforming information into an intelligence product for distribution to the policy maker (Classen, 2005:153; Shulsky & Schmitt, 2002:41). Furthermore, it is the driving force behind collection through the identification of information gaps and subsequent re-tasking (Clark, 2013:59; Gressang, 2007:137). The task of the analyst is to contextualise the information and ascertain its implications for national security. If information is collected and not accurately interpreted and collated into a product, the information will have no use for the policy maker. Furthermore, analysts are faced with the

challenge that they are dependent on the collectors for information. If they do not receive useful information from the collection process, the analyst cannot produce an intelligence product and the client cannot be informed about security issues.

The intelligence product is compiled from all sources of information and is the outcome of the intelligence process (collection and analysis). The type of product disseminated to the client will depend on the urgency and the nature of the situation. The products may range from a written report to a verbal report and can be clustered into three groups: current intelligence (providing timely warning), basic intelligence (providing and in-depth analysis on a specific issue) and intelligence estimates (providing an analysis on an event as it plays out and what might be expected in future) (Classen, 2005:85; Kent, 1966:25; Shulsky & Schmitt, 2002:57). These products differ in various ways. First, the products vary in length. Current intelligence is the shorter product, containing a short to-the-point message. The intelligence estimate on the other hand is a longer document with detailed analysis about the event. The second important difference is the focus of the product (Classen, 2005:85; Lowenthal, 2006:61; Shulsky & Schmitt, 2002:57). Current intelligence products focus on issues that immediately need the attention of the client. Longer products are concerned with trends and strategic issues that do not need the immediate attention of the policy maker. These classifications may vary from one intelligence service to the other, depending on the priorities of the organisation. Furthermore, analysis is also responsible for assisting the collection process with the compilation of requirements. This product is compiled by the analyst and guides the collection process in relation to specific needs with respect to an intelligence priority. Another important aspect of the analysis process is feedback in relation to the collection process. It is not only the feedback from the client with regard to the usefulness of the final product that is important, the feedback with regard to the usefulness of the raw information from the collection process is equally important. The feedback together with the tasking, guide the collectors to obtain the relevant information.

For the purposes of this study, analysis is the evaluation, interpretation and collation of raw information into an intelligence product to be disseminated to the client for use in policy formulation or reformulation. Furthermore, the analyst drives and guides the collection process through requirements, identifying information gaps and continuously providing feedback to the collection divisions. It is imperative that the analysts play a significant role in determining key priorities and guide collection through regular feedback, since they receive all relevant information and have the full picture. While the product of the analysis process is disseminated to the client to support the policy formulation process, the guidance to the

collection process is equally important. Feedback and guidance to the collection process ensure that correct information is collected to enhance the intelligence product to the client. Collection and analysis can be viewed as the essence of the intelligence process. However, other elements are needed to support this process and one such element is counter-intelligence (CI). The next section focuses on CI as an important supporting function.

5.3.3 Counter-intelligence

Although CI is not included in the traditional intelligence cycle, it is a very important supporting function of the intelligence process. While CI is a function of intelligence, it should not be viewed in isolation. It is a function that safeguards the entire intelligence process. In this regard CI can be described as the protection of a country's intelligence operations, actions and information against other states or foreign entities (Lowethal, 2006:145; Shulsky & Schmitt, 2002:99).

Lowenthal (2006:145) mentions three types of CI: collection of information relating to other intelligence services; defensive CI, preventing actions of hostile intelligence services; and offensive CI through the identification of hostile activities and using these activities against the opposition (e.g. false information). With regard to South Africa, the General Intelligence Laws Amendment Act (11 of 2013) (South Africa, 2013:2) describes CI as "means, measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct (security screening) vetting investigations and to counter (subversion, treason, sabotage and terrorism aimed at or against personnel, strategic installation or resources of the Republic) any threat or potential threat to national security".

CI is an important element of the intelligence process. It ensures that the intelligence community can operate within an environment free from espionage. With regard to this study, CI can be defined as the defensive and offensive actions and operations undertaken to protect a country's secrets against other states or foreign organisations. CI supports the intelligence process with two actions. First, it includes preventative or defensive actions to prevent the opposition from obtaining valuable intelligence. Second, it plays a mitigating or offensive role when the opposition or enemy has already gained access to secret information.

While collection, analysis and CI are elements maintained by most intelligence organisations, the final element of covert action is controversial. Not all intelligence services

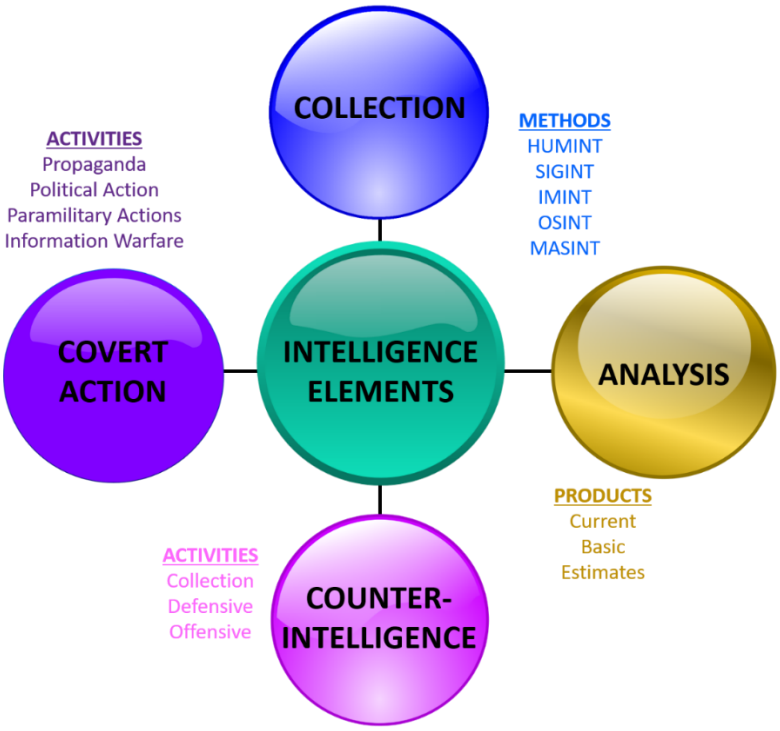
subscribe to this function. However, for the sake of completeness, the next section focuses on the issue of covert action as the final element of intelligence.

5.3.4 Covert action

Covert operations are mainly secret operations of one country in pursuit of its foreign policy objectives to influence political, economic or military conditions in another country (DCAF, 2003:3; Johnson & Wirtz, 2015:225; Lowenthal, 2006:157; Shulsky & Schmitt, 2002:75). Activities within the field of covert action include propaganda, political action, paramilitary activities and information warfare (Johnson, 2007:xii; Lowenthal, 2006:162–165). These actions can be used together or separately to reach the desired goal.

Covert action is one of the most contested intelligence functions, mainly because these secret actions take place in another country without the knowledge of the host country. These actions are viewed as unlawful and intrusive of the sovereignty of other states. Furthermore, it is in contravention of the international law principle of "non-interference". Covert actions present moral problems for a wide range of people because of the use of deception, sometimes violence, and secrecy (Finan, 2010:1). There is a conflict between these moral values and national security or national interest. As of late, covert actions are increasingly being disputed as an appropriate function of democratic intelligence services (Caparini, 2007:3; Church, 2011:233–237; Finan, 2010:1; Lowenthal, 2006:157). The South African White Paper on Intelligence (1995:7) pronounces as follows on covert actions: "Measures designed to deliberately interfere with the normal political processes in other countries and with the internal workings of parties and organisations engaged in lawful activity within South Africa, must be expressly forbidden. Intelligence agencies or those within them guilty of such breaches must be disciplined in the severest terms". South Africa's position on the issue of covert action is clear and the intelligence service does not subscribe to such actions.

For the purposes of this study covert action is described as a foreign policy instrument to influence and manipulate events in another country without the knowledge of that particular country. These actions are incompatible with the values of a democratic society and it is for this reason that is not legal within the South African context.



Source: Own construct

Figure 40: Intelligence elements

All these elements are depicted in Figure 40 above. This figure illustrates the four intelligence elements, nameley collection, analysis, CI and covert action. These functions of intelligence have developed over time and were expanded and institutionalised when intelligence organisations formed in the second half of the 19th century (Herman, 1996:15).

Against this background, the subsequent section explains the evolution of intelligence and its elements. Furthermore, the role of technology in the development of intelligence is clarified.

5.4 The evolution of intelligence

Espionage or spying, as it was known earlier, is an ancient profession that has been an integral part of war throughout the ages (Kent, 1974:5). The terms intelligence and espionage are often used interchangeably. However, the meaning differs greatly. According to Troy (1991:443–444), the starting point for understanding intelligence should be the profession of the “spy”, which translates into spying or espionage. Lerner (2004:412) views espionage as “the use of spies, or the practice of spying, for the purpose of obtaining information about plans, activities, capabilities, or resources of a competitor or enemy”. As indicated in the previous section, intelligence organisations only became official during the

second half of the 19th century (Herman, 1996:15). Since then, intelligence organisations and practices have grown into familiar institutions.

The profession of intelligence has evolved from spying to espionage, and today the word intelligence is preferred when referring to this ancient occupation. The section below highlights the different periods in the development of intelligence and the most important technology advancements that affected intelligence for each period.

5.4.1 Intelligence: early history

With this brief introduction above, the first discussion focuses on the early history of espionage (as it was known then). The discussion is divided into ancient times and the Middle Ages.

Ancient times (2000 BC to 1000 AD)

Espionage or spying is often referred to as the second oldest profession. According to Dulles (1965:11), the earliest sources of intelligence were prophets, seers, oracles, soothsayers and astrologers. The first reference to spies is found in the Bible, Numbers 3:1, when Moses sent out 12 men to explore Canaan. Another case is found in Joshua 2:1, where Joshua sent two spies to Jericho to determine their military strength. Sun Tzu's *Art of War* is one of the most cited sources on ancient espionage. The *Art of War* was written in around 500 BC and comprised 13 chapters, with Chapter 13 titled "Employing spies". Sun Tzu was the first writer in history to emphasise the importance of espionage (Burds, 2011:12). This ancient way of applying this profession is still used today. Intelligence services have a more sophisticated intelligence network that includes a variety of sources. However, the human sources remain an important part of the collection process.

In ancient times the main driver of espionage was the wars among regional rivals, while the key focus was on security and preservation of ruling regimes. Even during this time the issue of political power and strength was of great importance and the most significant role players were the Egyptians, Greeks and Romans. Their power was mainly seated in the military capacity of the regime. These regimes had to compete for resources and needed information about competitors' military strength and capacity. Sheldon (2003:4–5) is of the view that intelligence activities were an important part of the ancient regimes' "tradecraft", which was used as a tool to obtain information to make educated decisions. Great emphasis was placed on information obtained from human sources. Sun Tzu (Cleary, 1988:165) made the observation that foreknowledge can only be obtained by people who know the conditions of

the enemy. Together with the importance of HUMINT, the most important methods used to obtain information included written communication through codes and trick ink, surveillance through human sources (traveling traders, sailors, merchants), deception (Trojan horse), semaphore (Greeks), hidden compartments and the infiltration of problematic organisations (Lerner, 2004:416).

Middle Ages – 5th to the 14th Century

The need for espionage increased during the Middle Ages as political power increased. The most important political developments in Europe during this time were the formation of large nation states (France and England) in the 9th and 10th century and the rise of the Catholic Church in the 11th century (Lerner, 2004:417). During this time the emphasis of espionage was on the security and the preservation of the nation states and the Catholic Church (Lerner, 2004:417). As was the case in ancient times, regimes continued to compete for resources and expand their rule into other territories. It was imperative that information be obtained about the competitors' military capabilities. This was done mainly by using human sources. HUMINT continued to be the most important source of information in this period. However, this period was also the start of the diplomatic environment, which expanded the source alternatives for collecting intelligence. The large nation states operated within a diplomatic environment where messages were carried between the states by couriers. This created the perfect opportunity for intelligence gathering by intercepting messages. The peaceful situation of the nation states era was followed by the less peaceful rule of the Catholic Church. This period was characterised by the Crusades (military movement to take back Jerusalem) and the Inquisition (prosecution of anti-clericals), mainly aimed at solidifying the powers of the church (Lerner, 2004:418). This timeframe still involved networks of informants to obtain information about dissidents or planned actions against the church (Kent, 1974:14; Lerner, 2004:418). Although the church realised the importance of information obtained through espionage, no attempts were made to create or to build a formal intelligence organisation (Kent, 1974:14). Espionage continued to take place without a formal structure or formal rules and regulations. The focus was on secrecy and the lack of a formal organisation implied that the government or a governing body had deniability when activities were made public.

Even though espionage was not organised into a formal structure during this time, the activity of spying was used by governing bodies from the early ages. Human sources have always been used to obtain information. However, other forms of collection surfaced as communication methods developed. The interception of written communication started when couriers were used to convey messages between states. The priorities of collection were to

obtain information about the strength of the enemy and to identify individuals who were against the establishment. Although the profession was not formalised into an organisation, the activities continued to assist decision makers in the state and the church. This information was used to take political decisions.

The discussion focused on the early history of espionage. During this time technological developments did not play a role in the development of espionage. The next section emphasises the development of espionage during the Renaissance, with a focus on the main technological driving forces.

5.4.2 Intelligence during the Renaissance (14th–17th centuries)

The Renaissance started in Italy in 1350 when Italian scholars, scientists and artists formed a cultural movement based on a return to classical sources of learning. This was the start of the modern era. The movement spread to the rest of Europe and continued until the 17th century. According to the Concise Oxford English Dictionary (2004:1217), renaissance means a "revival or renewed interest in something".

Classen (2005:14) regards the period from the beginning of the 15th century to the end of the 18th century as "very important" in the evolution of intelligence. He substantiates his claim by highlighting the following driving forces that contributed to this evolution process:

- Rise of the nation states: During this time the government model in Europe moved away from being church-dominated to being nationalistic with the nation state (especially England with the monarchy) and the city state as the most important political role players (Lerner, 2004:418). As these nation states and city states grew stronger and richer, the competition for trade and exploration of the "New World" increased. This also necessitated an increase in espionage to have the competitive edge. The main aim of espionage during this timeframe was to protect political, military and economic interests.
- Diplomacy: Diplomacy is an integral part of governments' modern information gathering strategy. This initiative was started by Italian city states and was institutionalised in Europe in the 16th and 17th century, when permanent embassies where established in foreign capitals and were viewed as government's organisations for the collection of foreign intelligence (Herman, 1996:9–12). This can be regarded as the birth of the intelligence organisations. However, it was not until the mid-nineteenth century that more permanent intelligence organisations with more specialised capabilities were established (Herman, 1996:15).

- Growth of “secret intelligence”: The opening up of embassies and the placement of diplomats in foreign capitals increased diplomatic traffic. Information gathered through diplomatic means was transmitted through codes and ciphers back to the capital. This also provided the opposition with an opportunity to intercept and decode diplomatic communications (Classen, 2005:14).

Classen (2005:14) identifies the rise of the nation state, diplomacy and the growth of secret intelligence as important driving forces during this time. However, for the purposes of this study, technological developments are included as another driver and major advancement during the Renaissance. These technological developments influenced espionage and included invisible ink, encryption and telescopes (Lerner, 2004:419). Such developments made it easier to communicate and to obtain information about the enemy.

This period in intelligence history can be viewed as the renaissance of modern diplomatic intelligence collection. The foundations were laid for the collection of intelligence in a foreign country using the cover of the embassy. This development complemented the collection process through human sources. Furthermore, analysts could verify information obtained from human sources with information received by diplomatic means, increasing the reliability of the information.

This period was the starting point for the use of technology within the intelligence environment. However, the industrialisation period that followed and the resulting technological developments had a more significant impact on intelligence, especially with regard to surveillance.

5.4.3 Intelligence during the period of industrialisation (18th–19th centuries)

The Industrial Revolution, which started in Britain and quickly moved to the United States of America and Western Europe, took place in the late 18th and early 19th centuries. This phenomenon was mainly a result of the advancement in the technologies of industry and ignited the change from a mainly agrarian to an industry- and machine-dominated economy.

While the Renaissance laid the basis for diplomacy intelligence, the industrialisation laid the foundation for intelligence and modern technology application. Lerner (2004:419) describes the industrialisation as “the birth of modern espionage” and the beginning of technology in intelligence. Classen (2005:17) concurs and is of the view that this time period is “an

important chapter in the evolution of intelligence". Various important driving forces can be identified for the evolution of intelligence during this period:

- Competition: The competition between rival colonial powers for economic and territorial expansion resulted in numerous conflicts and wars (Classen, 2005:17; Lerner, 2004:419). This resulted in a demand for information on enemy positions and military strength. Although this competition was present since the middle ages, it intensified during this time as rivalry increased. Information or intelligence about enemy strength was of utmost importance.
- A temporary swing from secret to overt intelligence: The availability of foreign information increased as a result of the development of the printing press and the liberalisation of press and publication laws (Classen, 2005:18). This opened up the possibility of using open source information for purposes of intelligence. The availability and access to information increased as the printing press became more sophisticated. This was a small-scale boom of information and can be viewed as the frontrunner for the information explosion in the internet and computer age. This upswing in the use of open source information was short-lived. By 1914 the diplomatic use of the telegraph increased the role of espionage and secret intelligence once again (Herman, 1996:22). It was not until the Cold War that intelligence organisations realised the importance of overt information again.
- Nature of warfare: Industrialisation transformed the nature of warfare with the development of improved weaponry, which increased mobility and amplified the possibility of surprise (Classen, 2005:17; Herman, 1996:16-25). Therefore, more and better intelligence regarding rival military movements and strategies was needed. The type of intelligence needed regarding rivals included troop movement, weapon procurement and technological capabilities. A more sophisticated intelligence was needed, implying an improved technological capacity to obtain this intelligence.
- Establishment of intelligence organisations: In order to organise much-needed intelligence, military intelligence organisations were established during the second half of the 19th century (Classen, 2005:17; Debruyne, 2015:2; Herman, 1996:16–25). Intelligence organisations serve central government and are accepted as a permanent part of its bodies (Herman, 1996:3–4). According to Kent (1966:69), intelligence is "an institution; it is a physical organisation of living people which pursues the special kind of knowledge at issue". Kent (1966:69) underlines the following features of this organisation: must be prepared to do foreign country surveillance; must be able to explain past, present and possible future activities; the information produced must be

relevant, timely and complete in order for the policy maker to take action; and must have a staff of experts who are fully versed in the foreign policy objectives of the country and who are aware of and understand the strategic problems facing the country. Intelligence organisations started with a mainly military focus. However, as global threats evolved, the need for intelligence organisations with a broader focus increased. The mandate and scope of intelligence organisations differ from country to country. It is dependent on foreign policy objectives, security threats and government system. According to Van den Berg (2014:41), the classical structure of an intelligence community consists of the following organisations: a foreign intelligence service; an internal security service; technological services for government communications; a military intelligence structure; a police intelligence structure; a foreign affairs/relations department; and a joint intelligence coordination body.

- Development and improvement of the transport sector (Classen, 2005:17): This development had a positive influence on espionage. It was specifically the rail transport that made it easier for intelligence operatives to travel and be disguised as tourists. The transport development increased the scope of intelligence collection.
- Development of technology: With regard to technology, two specific developments had major effects on intelligence in general and collection in particular. The first of these inventions was the daguerreotype[26] (first practical form of photography) invented in 1837. This technology portrays everything exactly as it is. This was the best way of copying and transmitting information until the digital era. The second important development was the Morse code. In 1844, Samuel Morse transmitted the first message via wireless telegraphy. Governments could now send messages to embassies and to other states via telegraph. However, this provided rival services the opportunity to learn to tap lines to gain access to secret communications. These developments had an important impact on transmitting intelligence and the collection of information.
- Tradecraft: During this time period tradecraft was also transformed due to the development of various gadgets for concealment and transcription, making the transmission of secret information easier (Classen, 2005:17). The improvement in tradecraft assisted the handler (intelligence member responsible for obtaining information from the source) and the source (person providing information or intelligence) and made transmission without detection easier.

[26] The daguerreotype, named after the inventor, Louis Jacques Mandé Daguerre, was the first commercially successful photographic process (1839–1860) in the history of photography. It is a unique, accurate, detailed and sharp image on a silvered copper plate. Daguerreotype is different from photographic paper in that it is not flexible, it is heavy and must be kept in a special housing because it is breakable (http://www.daguerreobase.org/en/knowledge-base/what-is-a-daguerreotype).

During this era various important driving forces played a crucial role in the development of intelligence. The most important aspect would be the establishment of military intelligence organisations, which resulted from the need to coordinate military information and military actions. This is viewed as the front runner for the modern intelligence services. The creation of military intelligence organisations strengthened the government's capacity to obtain intelligence on military issues. Together with the establishment of military intelligence organisations, the most important technological contribution of this era was the development of the Morse code. This made transmission of information easier and inspired the skills of interception.

The establishment of the military intelligence organisations and the Morse code had profound implications for the intelligence evolution. These developments played a crucial role during World War I and II. The military organisations improved coordination, while the Morse code enhanced communications between the military forces. The next section elaborates on espionage during World War I and II.

5.4.4 Intelligence and the role of technology during World War I and II

Information and knowledge of intelligence during World War I is limited, mainly as a result of the destruction of archives during World War II. However, despite this reality, World War I can still be viewed as the beginning of the realisation of the importance and usefulness of intelligence. This can mainly be attributed to the technology developments towards the end of the 19th century, inter alia radio telephony (developed towards the end of the 19th century), aviation and photography. These technologies were introduced and put to the test during the World War I (Kahn, 2006:84). Kahn (2006:84) explains that "Intelligence did not have a major impact on war and politics until communication intercepts in Wold War I helped generals to win battles – a trend that continued in later conflicts". For intelligence to help a country win wars, it should be timely, reliable and effective. Debruyne (2015:1) is in agreement and is of the opinion that World War I was not restricted to a struggle on the battlefields, but also included an aggressive engagement of intelligence services.

Collection is an important element of intelligence and even more crucial during times of war. Kahn (2001:84) highlights that intelligence is not a primary element in a war. However, it is an important component that can help win a war. Various collection methods were used during World War I. These methods included information from combat units themselves (while in the field valuable information is gathered about the enemy and its combat

methods), captured prisoners, agent networks (HUMINT) and interceptions of enemy communications (SIGINT) (Ferris, 1988:25).

A mixture of old and modern communication methods was used during World War I, including carrier pigeons, dispatch riders, telephone and wireless telegraphy (transmission of Morse code) (Bruton, 2014:1). Although message interception has been taking place for centuries, the intelligence obtained from these messages could not always be transmitted quickly enough to be useful. This situation changed during World War I with the use of radio transmissions. During World War I communication through telephone systems and dispatch riders proved to be difficult because landlines were damaged and messengers were killed. In order to maintain communication with front line units, the different armies were forced to introduce radio and field telephones. This new method of communication not only provided the sender with quick transmission, but it also provided the enemy with a new opportunity for intercepting of messages and quickly transmitting it to the necessary client for use. This gave intelligence the opportunity to provide relevant, accurate information on time and in this manner assist with battles. The timeliness, reliability and effectiveness of intelligence were amplified with the use of SIGINT during World War I and II, influencing the outcome of both the wars. Even though various collection methods were used, SIGINT proved to be the most successful. For this reason, Ferris refers to World War I as the "dawn of modern signals intelligence" (1988:25). Historians claim that cryptographic intelligence shortened the conflict by two years and played a crucial role the victory of the Allied forces in World War II (Kahn, 2006:132; Murray, 2002:1).

The successful use of SIGINT during World War I paved the way for its use during World War II and played a crucial role in determining the outcome of the war. During the inter-war period the Germans started to use the Enigma[27] for military communication purposes. It was during this time that the Polish secret service managed to break the codes of the Enigma. At the beginning of World War II the Poles provided this information to the British, who continued research on breaking the codes. As every large war has its significant characteristics, Lewin (1981:501) was of the opinion that SIGINT was the principal theme for World War II. It is apt to consider World War II as the start of information warfare. This was a new type of warfare that advantaged the side with the best crypto analysts. Both the Allied forces[28] and the Axis[29] employed experts to decipher intercepted messages. The analysis of

[27] The Enigma is a machine developed by the Germans in the early to mid-20th century to protect military and diplomatic communication.

[28] Main powers within the Allied forces included Great Britain, France, Russia and the United States of America.

the messages also provided information with regard to the location, frequency, length and time of the transmission (Ferris, 1988:25; Lewin, 1981:509). This information was also useful to the military forces and could be used during planning of missions.

World Wars I and II played a significant role in the development of intelligence. It is especially the technological developments of SIGINT that enhanced the role and function of intelligence. The technology development that started towards the end of the 19th century was successfully introduced during World War I and continued to be implemented during World War II. It is safe to assume that intelligence gathered through SIGINT technologies formed the basis for the outcomes of both the wars.

World War I and II firmly laid the foundation for the interdependent relationship between intelligence and technology. The next section explains the development of intelligence and technology during the Cold War period.

5.4.5 Intelligence and the role of technology during the Cold War

Just after the devastation of World War II the United Nations[30] was formed with the sole aim of preventing another such event. It was both the Allied forces and the Axis's aim to not get involved in another such event. Sulick (2014:47) defined the Cold War as "an intense conflict that stops short of full-scale war". The Cold War can be viewed as an intelligence war between the Union of Soviet Socialist Republics (USSR) and the USA, focusing on espionage, counterespionage and technological surveillance. Both sides feared a surprise attack and in this war of information, the main aim was to obtain secrets through SIGINT, IMINT and HUMINT without being detected.

Both the USSR and the USA used HUMINT (recruiting of spies) to obtain crucial information on the other side's activities. However, the USA found it more difficult to recruit within the USSR because foreigners were monitored closely and contact with its citizens were restricted. Furthermore, the USSR's counter-espionage capabilities were more advanced, as the country already had the spying practices of the KGB (*Komitet Gosudarstvennoy Bezopasnosti* – the main security agency in the USSR from 1954) and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (also known as GRU).

---

[29] During World War I the Axis comprised Germany, Austria-Hungary and Turkey, while Germany, Italy and Japan formed the Axis during World War II.

[30] The Charter of the United Nations was signed on 26 June 1945 in San Francisco. According to the Pre-amble of the charter, it was formed to "save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind".

The USA on the other hand only established its first counter-espionage authority, the Federal Bureau of Investigations, in 1939, followed by the Central Intelligence Agency in 1947 (Sulick, 2014:48). Although the USA's intelligence organisations were relatively inexperienced, they did manage to recruit various spies during this period, most notably Dmitriy Polyakov, Adolph Tolkachev, Ryszard Kuklinski, Oleg Penkovsky and Yuri Nosenko. At the same time the USSR also had their spies, inter alia the Cambridge Spy Ring, the John Walker family of spies and Aldrich Ames (Sulick, 2014:48). The USSR also recruited spies in the UK: Kim Philby, Guy Burgess and Donald McLean (Kent, 1974:84). It is interesting that Julius and Ethel Rosenberg were the only spies in the United States that were executed during the Cold War.

The information received through HUMINT was complimented by technological intelligence that provided the necessary evidence about the enemy's capabilities and plans. The most important technological development during the Cold War was overhead reconnaissance (Sulick, 2014:48). Developments started with USA aerial reconnaissance flights intercepting military communications and photographing military facilities using the high-altitude U-2 aircraft. However, after a U-2 aircraft was shot down in 1960, this manner of collecting intelligence was abandoned. During this period both the USSR and the USA developed spy satellite capabilities that produced high resolution imagery of weapon capabilities on both sides.

Other important technology developments include the computer and the internet. During the Cold War computers played a crucial role in the design and production of nuclear weapons (Hecht & Edwards, 2010:288). However, the full extent of these technological developments was only felt in the post-Cold War era. Even though there where advancements in the technology field during the Cold War period, it is the opinion of the author that espionage methods moved back to relying on HUMINT rather than technological means. This is evident from the large number of spies that were captured during this period. The counter-espionage element of intelligence was developed extensively during this time period as both sides were well aware of the other's intentions and it was crucial to protect themselves against espionage activities. During this time, SIGINT capabilities were developed further by both the USSR and the USA. However, information pertaining to the use and application of SIGINT during the Cold War is limited because of the secrecy surrounding these activities. This information is not in the public domain to protect sources and capabilities.

While the Cold War began with the formation of the UN, it did not imply an end to espionage and intelligence activities. In fact, it intensified these activities, because both parties were

afraid of being left behind in military and technological developments. This era can be viewed as the beginning of the computer and its applications to the intelligence environment. Against this background the final section focuses on the post-Cold War period.

5.4.6 Intelligence and the role of technology in post-Cold War period

During this timeframe two developments can be identified that had major implications for espionage: first the end of the Cold War and second the ICT[31] revolution. When analysing the first development, namely the end of the Cold War, it is clear that, while the intelligence brief was clear and simple during the Cold War era (monitor USSR activities), the unexpected end of the Cold War created uncertainty with regard to intelligence priorities and targets. Subsequently, government intelligence organisations were downsized because the threat was perceived as no longer present (Campbell, 2013:46). Even though this process was reversed once the new security environment was conceptualised, it created a vacuum that was quickly occupied by private intelligence providers. For the first time, the intelligence community was in competition with the private sector in an area that was previously the responsibility of government.

The second important development is the growth in the ICT sector. The post-Cold War security environment, as sketched in Chapter 3, is characterised by new intelligence priorities and new role players. It was also explained that ICT was one of the main drivers of globalisation. Campbell (2013:57) is of the opinion that post-Cold War technology played a crucial role in intelligence transformation. Schwab (2016:11) refers to industrial revolutions[32] and he is of the opinion that the fourth industrial revolution started in the beginning of the 21st century. This revolution builds on the digital revolution (third industrial revolution – 1960 to 1990). However, the new revolution is based on an internet that is more powerful, integrated, global and mobile than the previous industrial revolution (end of the 20th century) (Schwab, 2016:11). This has created a fertile environment for new trends, which impact negatively on national security and therefore warrant the urgent attention of the intelligence communities. Intelligence organisations are engaged with the business of information and specifically the provision of actionable intelligence to assist the policy maker with regard to national security issues. It is not surprising that the major developments in the area of ICT during the post-Cold War era had a serious effect on intelligence organisations and their provision of

[31] For the purposes of this study the ICT revolution includes the computer, internet and mobile phone developments.

[32] The first industrial revolution (initiated by the construction of the railroads and development of steam engines) started around 1760 to 1840 and the second industrial revolution (initiated by the invention of electricity) from late 19th to early 20th century (Schwab, 2016:11).

intelligence. With regard to ICT, the most important development during the past 50 years has been the internet. Wettering (2001:342) believes that “among the many kinds of business for which the internet has proven to be a godsend is the espionage trade”.

This new security environment created by the end of the Cold War and the ICT development brought new challenges and opportunities to the intelligence community. These include the following:

- Intelligence competitors: One of the major challenges intelligence organisations are faced with is that intelligence is no longer just the domain of the government intelligence departments. Before the information age, government, and particularly the intelligence community, had control over the provision of intelligence. This situation has changed mainly as a result of rapid IT development. The intelligence organisations are currently competing with various private intelligence organisations (UK-based Oxford Analytica and Stratfor, and the Institute for Strategic Studies in South Africa), academics and the media. These organisations have access to funding and are not bound by bureaucratic rules and regulations.
- Virtual and borderless cyber world: Another challenge to the intelligence community is the new environment, which is no longer just the physical and detectable surroundings, but now also includes the virtual and borderless cyber or internet world. This cyber world has created a perfect environment for malicious actors to plan illegal activities across borders, while remaining anonymous (Campbell, 2013:61). The intelligence community is now faced with new threats, such as computer hacking to steal data, easy mobilisation of communities through social media and online terrorist activities such as planning, recruiting and fundraising. However, this environment also provides major opportunities to the intelligence organisations with regard to the collection process. Wark (2003:2) is of the opinion that the internet revolution had a positive impact on the use of OSINT. While Wark (2003:2) only mentions the use of OSINT, he also implies that collection has been made easier because information is more accessible through the internet. It is estimated that 90 per cent of all intelligence is collected through OSINT (Wettering, 2001:344). One of the least developed areas of OSINT is SOCMINT, which provides an abundance of information to the intelligence analysts. Schwab (2016:77) identifies social media as one of the emerging technologies that is currently transforming international security. The social media websites allow for the sharing of pictures, videos and personal information that provide valuable information if contextualised.

- Surveillance tool: The internet provides the intelligence community with the tool of surveillance. The USA Director of National Intelligence, James Clapper, acknowledged in February 2016 that intelligence agencies "might use a new generation of smart household devices to increase their surveillance capabilities". Clapper (2016:1) presented his Worldwide Threat Assessment of the USA Intelligence Community Report to the Senate Select Committee on Intelligence on 9 February 2016. The report indicates that cyber and technology developments are one of eight global threats facing the USA and that the Internet of Things (IoT)[33] is a major threat to cyber defence (Clapper, 2016:1). However, it also provides an opportunity to the intelligence community to harvest information with regard to surveillance, monitoring, location tracking and recruitment (Clapper, 2016:1). This information assists the analyst to create and maintain the intelligence picture.
- Information overload: Intelligence organisations are faced with the challenge of information overload. This situation is a result of the ICT revolution, which makes it difficult to discern between real intelligence and noise. Not all information is relevant and intelligence analysts should evaluate the information to determine its usefulness. For this reason, it is important to understand the motivation behind the production of information on the internet (Keohane & Nye, 1998:84). Keohane and Nye (1998:84) highlight the fact that the type and quality of information in cyberspace is more important than the quantity. They identify three types of information (Keohane & Nye, 1998:84). The first type of information is free information, which is information that is created and distributed without receiving or intending financial compensation (Keohane & Nye, 1998:84). This type of information has the main intention to influence the audience. The 2016 American presidential campaign is a very good example where information was used to influence political thinking in the USA. With this type of information it is important to evaluate the factual correctness of the content. Commercial information is the second type of information that is created and distributed to receive payment (Keohane & Nye, 1998:85). The last type of information Keohane and Nye (1998:84) identifies is strategic information, which is information that is of great use if the competitor is not aware of it.
- Presentation of intelligence products: Although technology mostly affected the collection methods of intelligence, it also changed the production of intelligence in that products could be presented more visually (Wark, 2003:1). The product is presented in a more user-friendly fashion by using visual aids such as interactive maps, pictures and videos.

[33] According to the Meola (2016:1), the Internet of Things (IoT) refers to the connection of devices (other than typical fare such as computers and smartphones) to the internet. Cars, kitchen appliances, and even heart monitors can all be connected through the IoT.

Furthermore, the intelligence product can be distributed to the client in a quicker and safer manner by using new technologies.

- HUMINT management: The internet is not only useful for open source collection, but is also an important tool for human source management. It is an easy and cheaper way of identifying, recruiting and communicating with sources (Wettering, 2001:345–349). The internet assists with the targeting process. A potential source can be identified with the assistance of the internet. Most people have an online presence in the form of a personal website or on social media websites. The information is overtly available and can be used for introductory purposes. The potential source can be based anywhere in the world. Once the potential source has been befriended, the next step would be recruitment. Internet communication makes this process very easy and the handler does not have to travel to the country where the source is based. Information can also be transmitted via the internet in a secure manner, such as through steganography (using large message to hide the intended message) (Wettering, 2001:348). The internet has the following advantages for the intelligence services: cost saving (operatives need not be in the country where the source is staying), security (electronic communication safer than personal contact) and speed (transmission of information is immediately available) (Wettering, 2001:358). Wettering (2001:359) is of the opinion that although internet spying is cheaper, it will not replace SIGINT or HUMINT. Wark (2003:3–5) argues that although technological collection is favoured above HUMINT, certain information such as perceptions is only accessible through human sources and therefore HUMINT will always have a role in the collection process. While the internet has made it easier for intelligence services to collect information, it has also opened up avenues for terrorist organisations (This aspect is discussed in greater detail in Chapter 7.)

The above discussion reflected on the challenges and opportunities that the end of the Cold War and the ICT had for intelligence. During this time there were also other technology developments that influenced intelligence, although not to the same extent as ICT. These include geospatial intelligence, which is the fusion of real-time imagery, GPS data and digital maps into Geographic Information Systems (Campbell, 2013:62).

In analysing the post-Cold War period, it is clear that two developments had major implications for the progress of intelligence. The first development or event is the end of the Cold War. This event had implications for the focus and priorities of intelligence organisations, which left the intelligence community without clear and focused priorities. The second development is the growth in ICT. The most important technology developments for this time period are the internet and mobile phone communication. These technologies

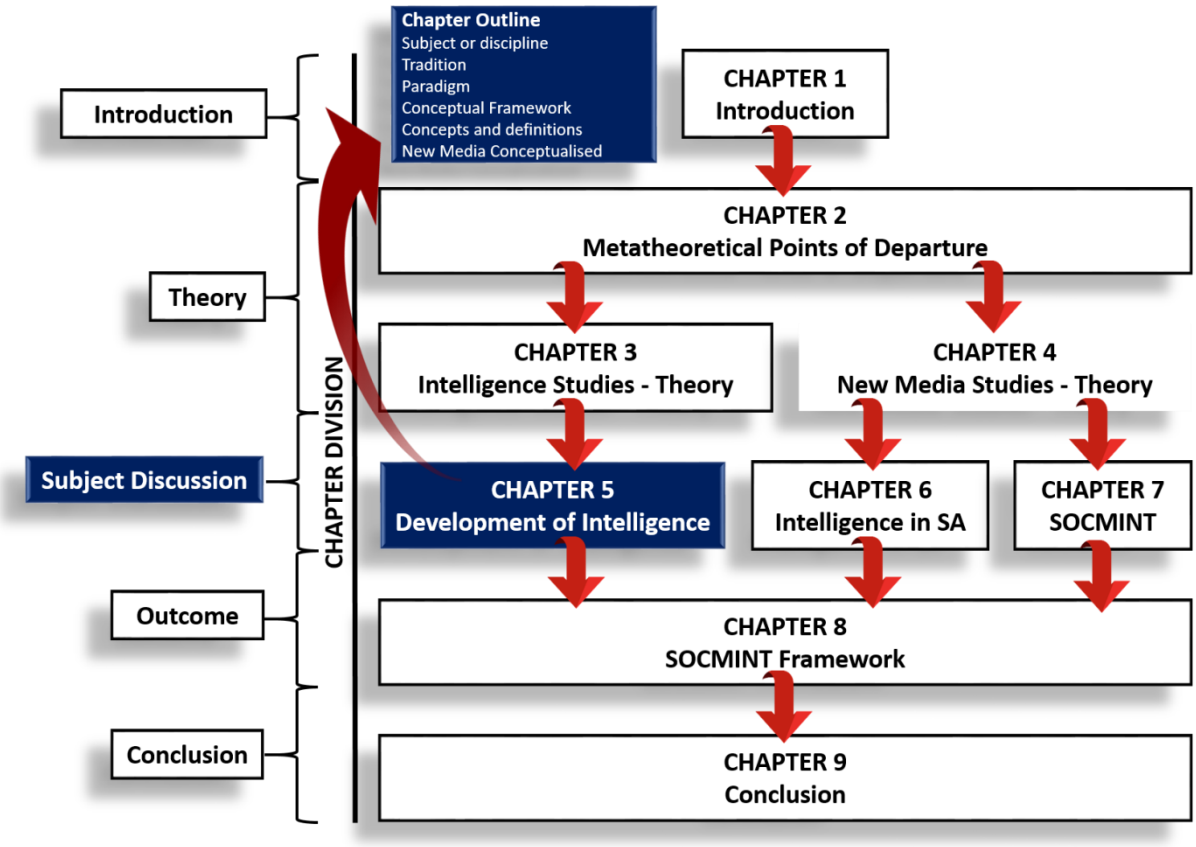
shaped a new borderless environment, creating new threats to national security with direct implications for intelligence services. The intelligence communities are faced with new targets and priorities as a result of the changes in the global environment. Furthermore, collection and analysis have to adapt to new technologies – ICT brought with it new collection methods and increased access to information that have to be addressed during analysis.

5.5 Conclusion

The main aim of this chapter was to explain the evolution of intelligence through the ages and the important role technology played in its development. It is important to highlight this issue as this study is a combination of intelligence and technology. Furthermore, it is vital to indicate where the SOCMINT phenomenon fits into the development of technology.

Figure 41 provides a summary of this chapter and indicates how it fits into this study. The chapter started with an explanation of the primary purpose, function and elements of intelligence. It is imperative to highlight these functions and elements as the development of intelligence directly affects them. The purpose of intelligence is to provide the government with information about threats and opportunities to protect national security. The development of intelligence affects the purpose as it improves the provision of intelligence to safeguard the country.

The chapter continued to discuss the key focus, the evolution of intelligence and the implications of technology development. The development and evolution of espionage was divided into seven timeframes: ancient times, the Middle Ages, the Renaissance, the industrial era, World War I and II, the Cold War and the post-Cold War era. Each timeframe was discussed with regard to the technology development and its implications for the evolution of intelligence. Initially the role of technology was insignificant. However, as the technology developments increased, its role and impact on intelligence became more noteworthy.



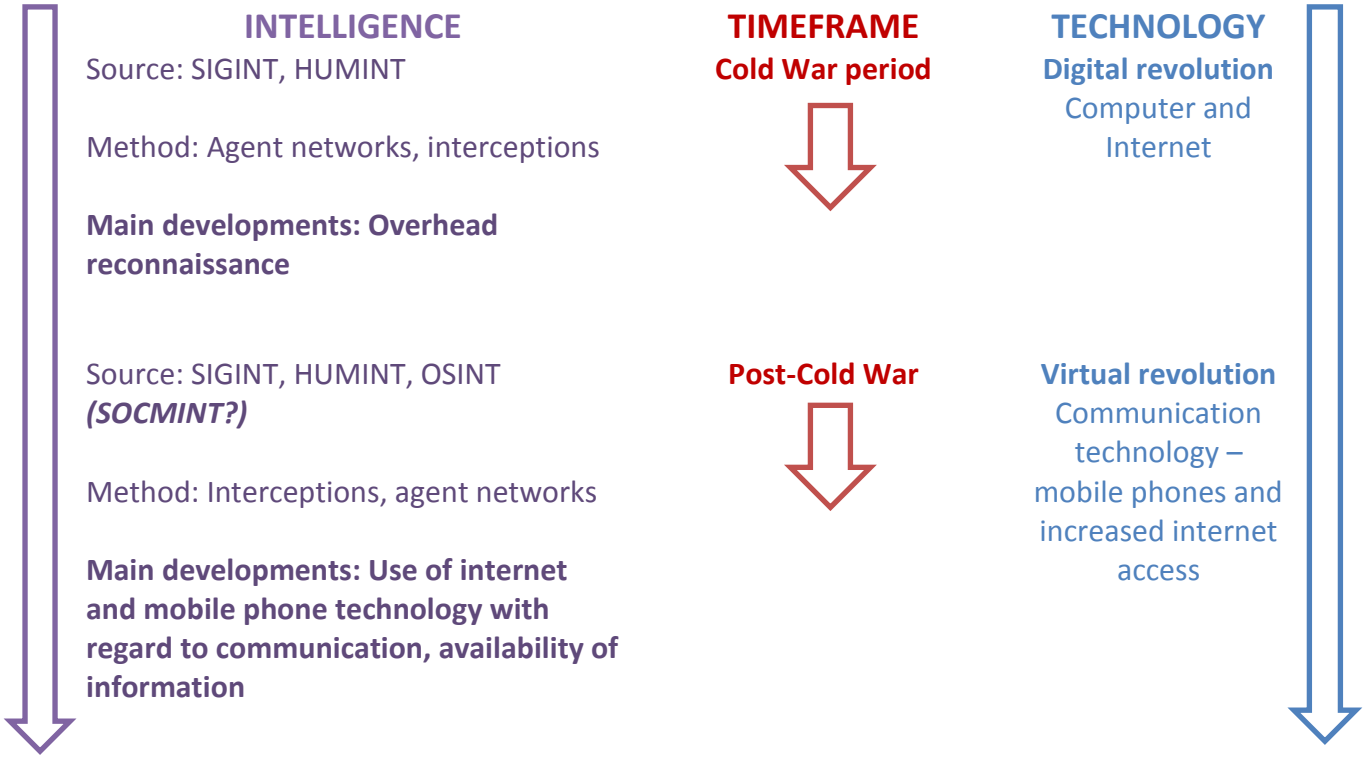
Source: Own construct

Figure 41: Chapter summary

Table 5 below summarises the developments of intelligence and technology during the various timeframes. The development of espionage began in the ancient period. However, during this time the main form of espionage was focused on interception of written messages transported by couriers. Technology started to influence intelligence on a small scale during the Renaissance period when remote surveillance was made easier through technologies such as the telescope. During the industrial era technology developments such as rail transport and the Morse code played a significant role in the use and development of intelligence. It was not until World War I that the importance of intelligence was duly noticed and appreciated, mainly as a result of the intelligence (SIGINT) obtained through the interception of technologies such as the radio. This continued through World War II. The ICT development started in the Cold War period. However, it was only during the post-Cold War period that it played a crucial role in the development of modern intelligence. It is especially the internet, computer and mobile phone technologies that fundamentally changed the intelligence collection process.

Table 5: Timeline: Intelligence and technology development

INTELLIGENCE	TIMEFRAME	TECHNOLOGY
Sources: HUMINT Method: Interceptions of written communications and agent networks **Main developments: Realisation of role of espionage**	**Ancient times**	
Sources: HUMINT and Diplomatic communication between Nation States Method: Interceptions of written communication and agent networks **Main developments: Diplomatic Interception between Nation States**	**Middle Ages** **5th -14th Century**	
Sources: HUMINT and Written Diplomatic communication between embassies Method: Decoding interceptions and sending coded messages through encryption **Main developments: Interception of communications from Embassies**	**Renaissance** **14th -17th Century**	Invisible ink Clocks Telescopes
Sources: HUMINT, diplomatic communications, photographic evidence from Daguerreotype Method: Interceptions of diplomatic communications trough wiretapping, Daguerreotype **Main developments: Establishment of military intelligence organisations and wiretapping**	**Industrialisation** **18th – 19th Century**	Morse code Telephone and fax machine Transport infrastructure Daguerreotype
Sources: SIGINT and HUMINT Methods: Interceptions and Agent networks **Main developments: Interception and code breaking capabilities – SIGINT**	**World War I and World War II**	**Analogue revolution** Radio



Source: Adapted from Van Den Berg, 2014:18

When analysing the evolution of intelligence over all the timeframes, various aspects can be highlighted:

- Two timeframes stand out as the most important. The first is World War I and II. This time marked the start of the use of SIGINT. This technology played an important role in emphasising the important role intelligence can play in a war situation. SIGINT played a crucial role in the outcome of the Wars. The second timeframe is the post-Cold War period that started the digital communication era.
- Although other methods of intelligence collection have developed over the years, HUMINT remains an important choice for collecting information. One reason for this occurrence is that human sources can provide emotional information that cannot be provided by technology.
- Access to information increased over the years as technology improved.
- The skill sets intelligence organisations need have increased as technology development improved.
- The virtual revolution has created a new source of information called SOCMINT. This new information source is not utilised to its full potential within the intelligence environment. SOCMINT is discussed in detail in Chapter 7.

This chapter clearly shows how technology enhanced the development of intelligence and the reliance of intelligence on technology. Technology is such an important part of daily life, it is imperative to learn how to apply it within the intelligence environment and to learn how to manage its consequences. It is important to take Wark's (2003:1) warning on board, that "one thing seems clear: Learning to live with an open-ended 'war on terrorism' will mean learning to live with intelligence". Furthermore: "Technology will continue to be the driver of change" (Wark, 2003:6).

With this chapter as basis, it is important to conceptualise the South African intelligence environment. The next chapter addresses the South African intelligence history and explains the role of technology in these developments.

CHAPTER 6: THE HISTORY AND DEVELOPMENT OF INTELLIGENCE WITHIN THE SOUTH AFRICAN CONTEXT

In the world of espionage the normal rules are not applicable. Everything is allowed in the name of national security – even to talk to the country's number one enemy.
Dr N Barnard (2015)

6.1 Introduction

It is apt to start this chapter with a quote from Barnard, as he and NI played an important role in influencing and changing the political and the intelligence dispensation within the South African context.

Chapter 5 highlighted various important historical political events that took place around the globe. The chapter also highlighted various significant communication technology developments that stimulated the evolution and growth of intelligence. These global events also affected the political developments in South Africa and therefore also the intelligence progress in the country. However, even though global political events influenced the political development of South Africa, two other important realities also shaped the political landscape of the country. These include its geographical position on the African continent and its strategic resources that made it attractive to global role players.

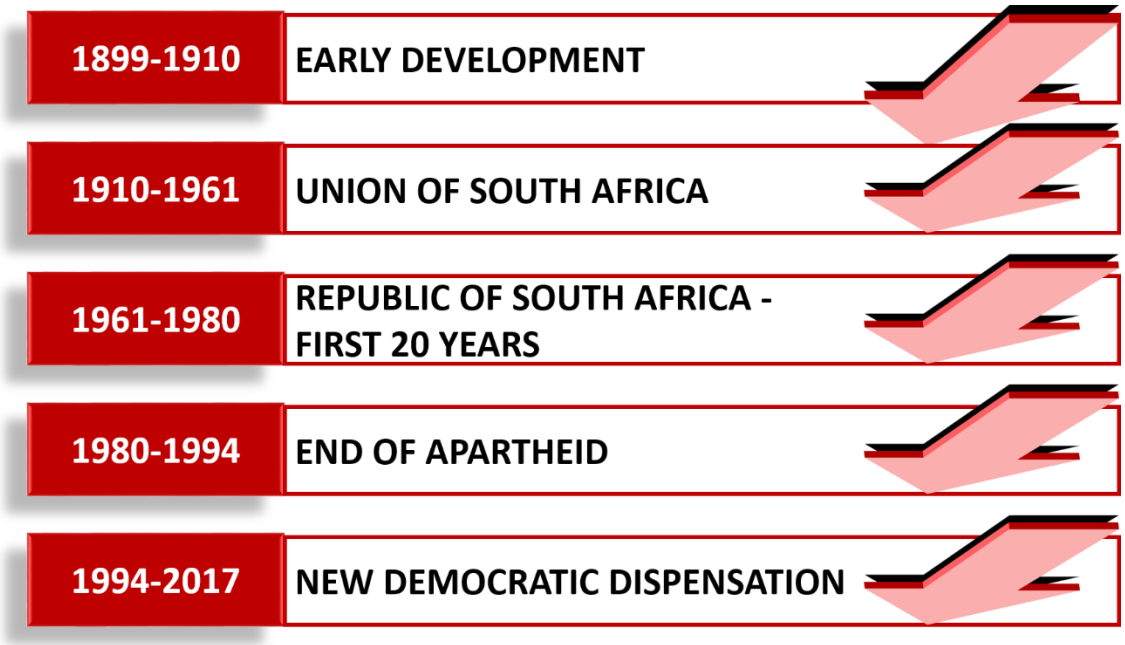
Just as it was necessary to highlight the world history of intelligence, it is important to discuss the history of South African intelligence to understand the current intelligence dispensation. However, the history is not addressed in great detail, main events are highlighted and their role in intelligence development in South Africa is explained. With regard to technology, the development in South Africa followed the same lines as in the rest of the world as explained in Chapter 5.

It was mentioned previously that intelligence is a very young academic field. However, this is even truer for the South African context. Information regarding the early history of intelligence in South Africa is limited. The main reason for this is the secret nature of the profession. Some documents are available from previous intelligence practitioners, written in response to journalistic writings. Swanepoel's (2007) *Really inside BOSS: A tale of South Africa's late intelligence service* is such a case in point. This book was written in reaction to *Apartheid's friends: The rise and fall of South Africa's secret service* by James Sanders

(2006). In his book Swanepoel (2007:1) tries to refute some of the allegations and claims made by Sanders with regard to the early intelligence services in South Africa, in particular Bureau for State Security (BOSS). One of the most detailed and comprehensive books about the South African intelligence services was written by O'Brien, *The South African intelligence services: From apartheid to democracy, 1948–2005* (2011). This book provides detailed discussions on the developments during various phases of the South African history. However, O'Brien (2011) was not an intelligence practitioner and the book should be viewed in this light.

The progress of South African intelligence is closely linked to local political events and developments. This can be connected to the purpose of intelligence (explained in Chapter 5), the policy process, the government of the day and its priorities and goals.

As explained earlier, the purpose of this chapter is not to have a detailed discussion on the evolution of intelligence in South Africa. The main purpose of this chapter is rather to highlight the main events in the development of intelligence and to focus on technological development during these phases. The discussion is structured according to the main political events in the South African political arena to examine how they influenced intelligence developments (Figure 42).



Source: Own construct

Figure 42: Timeline of political events in South Africa

The discussion highlights the intelligence focus or priority of each period, the intelligence tradecraft that was used most, and the most relevant technology applied. The chapter concludes with a brief discussion of the technological developments within the intelligence community. This is important as the next chapter focuses on communication technology developments, specifically as they relate to social media.

With this brief introduction as background, the first timeframe that is discussed is the early development of intelligence in South Africa from the late 1800s to 1910.

6.2 Early development (late 1800s to 1910)

The art of espionage was applied in one way or another by various groups in South Africa since 1652. However, for the purposes of this study, the description of intelligence development within the South African context commences with developments in the late 1800s. The discussion begins with the timeframe just before the first Anglo-Boer War. During this time the two Boer Republics (The South African Republic or Transvaal and the Orange Free State) had a limited intelligence capacity mainly aimed at the British (O'Brien, 2011:13). It was during the first Anglo-Boer War (1888) that President Paul Kruger requested the services of an experienced telegrapher from the Amsterdam Telegraph Department (Fordred, 1997:63). The telegrapher trained local telegraphers in receiving and sending messages in Morse, telegraph and heliograph (military signals trade). The Boers were in possession of an established field telegraph department (Fordred, 1997:63). During this time the Boers used fixed line[34] communications and the heliograph (Harris, 1998). These lines provided the Boers with a communication system using either the telephone or telegraph.

In 1889 President Paul Kruger appointed Dr Willem Leyds[35] to the post of State Secretary with the main goal of protecting the Boer Republics against the military operations of the British in the Cape Colony (Kamffer, 1999:41; Swanepoel, 2007:2). Leyds performed these tasks, and it was not until December 1895 that De Geheime Dienst[36] of the South African Republic was officially inaugurated as part of the detective branch of the South African Police (Kamffer, 1999:52–55). In order to perform this task (Vincent & Buranelli, cited by Swanepoel, 2007:2), Leyds recruited a group of spies and he devised codes and ciphers to

[34] Permanent communication lines were installed along all railway lines within South Africa prior to 1899.

[35] Dr Leyds, a Dutch lawyer, was the State Attorney from 1884–1889, State Secretary from 1889–1898 and Envoy Extraordinary and Minister Plenipotentiary of the South African Republic in Europe from 1898–1902.

[36] For a detailed study on De Geheime Dienst, see Kamffer's "Om een scherpe oog in's zeil te houden: De Geheime Dienst in die Zuid Afrikaanse Republiek", 1999.

communicate relevant information. In addition, Leyds also attempted to change foreign perceptions by funding foreign press in Europe who favoured the cause of the Boers (Kuitenbrouwer, 2012:60; Swanepoel, 2007:3). Leyds set up a press office in Paris to counter the British press conglomerate, Rhodes (Kuitenbrouwer, 2012:60). In the previous chapter these actions were described as covert actions for the purposes of propaganda. It is not known whether Leyds' actions actually increased sympathy towards the Boers. However, according to Kuitenbrouwer (2012:128), Dutch journalists published material from the war and played such a crucial role in the propaganda campaign that when the war broke out again in 1899, most journalists in France were supportive of the Republics. During the Second Anglo-Boer War (1899–1902) the Boers relied heavily on their own people to provide them with intelligence and resources (Van der Waag, 2015:38). Furthermore, it is assumed that radios captured from the British soldiers were used by the Boers in their own war campaign.

During the final stages of the Second Anglo-Boer War (occupation of Pretoria – 5 June 1900) the secret service of the Boer Republics collapsed mainly as a result of the invasion and the collapse of the state administration (Kamffer, 1999:382).

During this time, the intelligence focus was narrowly concentrated on information pertaining to the British forces and their movements and plans with regard to the Boer Republics. The technology (radios and war equipment) that was used by the British was far superior to those used by the Boers. However, the Boers had the strategic advantage in that they were familiar with the territory and this assisted the Boers in their war actions. Furthermore, the training they received from the Amsterdam Telegraph Department improved their communication skills. HUMINT was used extensively to obtain information about British movements. The propaganda war fought by Leyds is also a significant part of the efforts during this time and an important covert action example from the early history of South African intelligence. Leyds played such an important role in the South African intelligence history that the National Intelligence Service (NIS) honoured him by naming a hall after him, the Leyds Auditorium. This auditorium is still in use today. Even though the British won the war as a result of their superior technology and access to resources, they lost the support of the population. This was the start of Afrikaner nationalism.

Although the secret service of the Anglo-Boer War collapsed towards the end of the Second Anglo-Boer War, these developments contributed to intelligence progress in South Africa. This period laid the foundation for the establishment of future intelligence capabilities. The next discussion focuses on the period of the Union of South Africa from 1910 to 1961.

6.3 Developments during the Union of South Africa (1910–1961)

The Union of South Africa was established in 1910 and comprised the four self-governing colonies of the Cape, Natal, Transvaal and the Orange River. The unification had implications for the governing bodies of all four the colonies in general and law enforcement in particular. The government was faced with integrating different security cultures and was largely focused on the protection of the colonial regime and identifying anti-colonial resistance. Both the Police Bill and the Defence Bill were enacted in 1913, authorising the establishment of the South African Police (SAP) and the Union Defence Force (UDF) (Africa, 2006:71).

During the early stages of the Union, the British had influence over the intelligence developments in South Africa in the person of Sir Percy Sillitoe, who was MI5's contemporary director general (O'Brien, 2011:16–17). As a colony of Britain, South Africa's internal and external political and security environment was dominated by British priorities and models. This was also true for the domestic law enforcement and intelligence capacity. Both the SAP and the UDF established intelligence capabilities in the early 1920s (Africa, 2009:64; O'Brien, 2011:14). The 1921 Imperial Conference in London made South Africa responsible for maintaining order in the case of an uprising in Southern and Central Africa (Van der Waag, 2015:140). In an effort to ensure that they could adhere to this order, a full-time intelligence section within the Defence Force was established at Defence HQ (Van der Waag, 2015:140).

While the Defence Force was responsible for maintaining regional order (Southern and Central Africa), the South African domestic intelligence environment was the responsibility of the SAP, which reflected the British model of policing. The intelligence capacity within the SAP was developed around the 1920s and focused on internal security (O'Brien, 2011:14). The information was mostly supplied by informers and the focus was on anti-government security issues (Africa, 2009:64). During this time the Union did not have the capacity for foreign intelligence and was dependent on the British MI5 for international intelligence needs (O'Brien, 2011:14). The British intelligence organisations preferred this situation, as it gave them leverage over the South African intelligence structures.

Although the Union was part of Britain, the distrust between the Afrikaners and the English (resulting from the two Boer Wars) strained the relations between the two countries. Intelligence cooperation became more difficult as the political goals of the two governments increasingly diverged. The British were in a dilemma as they wanted South African

intelligence to develop along the same lines and standards as MI5 to grow an "anti-communist western intelligence alliance", but the internal political situation made it difficult (O'Brien, 2011:16–17). The Union was faced with a duality. On the one side there were forces who wanted to stay loyal to the British, while on the other side there were forces who wanted Afrikaner independence. This duality of the political situation within the Union complicated the intelligence environment. The security forces in the Union were also divided along the lines of anti- and pro-British Union rule and this resulted in the continued rivalry among the security forces. The SAPs was anti-British rule and the UDF was pro-British rule (O'Brien, 2011:14). For this reason, the British viewed the UDF as a better option to support in exchange for intelligence in relation to right wing Afrikaner activities in the Union.

This distrust increased as radical Afrikaner nationalists infiltrated security forces and shifted the focus to self-preservation. The SAP was heavily dominated by Afrikaners opposed to British Union rule and therefore the British were opposed to efforts by the Union government to develop and establish an autonomous intelligence capacity (O'Brien, 2011:14). However, the Union government started to develop its own capacity and established the SAP's Detectives Branch in 1938 with its main focus being counter-subversion and CI (O'Brien, 2011:14). The Branch was strategically established within the SAP that was opposed to British rule and could therefore focus on promoting the Afrikaner nationalist idea.

The expansion of the independence of the Union government was interrupted by the outbreak of World War II. During World War II the Union was faced with two distinct security challenges. The first challenge was the threat of external aggression as a result of World War II (Fedorowich, 2005:211). Due to the Union's affiliation to Britain it was aligned with the Allied forces. The second and much more pressing challenge was the pro-Nazi, anti-British right-wing Afrikaner groups such as the Ossewabrandwag and the Broederbond inside the borders of the Union (Fedorowich, 2005:211; O'Brien, 2011:15). Faced with these challenges, Smuts[37] attempted to establish a standing intelligence capability. He formed two intelligence structures at the defence headquarters (Fedorowich, 2005:213; O'Brien, 2011:16). The first was the creation of the position of Director of Intelligence in 1939 under the South African Chief of General Staff responsible for civil security, local censorship and propaganda (Fedorowich, 2005:213). The second structure was the Department of Military Intelligence (DMI – within the UDF), established in February 1940, responsible for all military intelligence and security, including censorship and propaganda while on active duty outside of South Africa (Fedorowich, 2005:213; O'Brien, 2011:16).

[37] Jan Christian Smuts was Prime Minister from 1919 until 1924 and then from 1939 to 1948.

With the outbreak of World War II the South African government appointed an Interdepartmental Cabinet Committee to oversee and make recommendations regarding internal security issues (Fedorowich, 2005:214; O'Brien, 2011:16). This committee comprised the Departments of Censorship, Military Intelligence, SAP, Railway Police, and Treasury, Immigration and Customs (Fedorowich, 2005:215; O'Brien, 2011:16). One of the main priorities was to curb subversive activities by pro-German groups. The Cabinet Committee proposed the establishment of committees in areas with large concentrations of German-speaking nationals (Transvaal, Orange Free State, Northern Natal and Eastern Cape) (Fedorowich, 2005:215). The main purpose of these committees was to monitor and report on hostile activities within these groups (Fedorowich, 2005:215). With all the various committees, the problem of coordination arose. Denys Reitz, then Deputy Prime Minister, raised the concern that there was "a great deal of overlapping and delay in regard to the collection and distribution of intelligence information" (Fedorowich, 2005:215). Smuts responded to this problem with the establishment of the Intelligence Records Bureau, which served as a "clearing house for the processing, recording and transmission of information" from the various departments (Fedorowich, 2005:214; O'Brien, 2011:16). This also provided an entry point or coordination mechanism for liaison with intelligence centres abroad such as Singapore, Nairobi, Cairo and London (Fedorowich, 2005:216). The problem of coordination and information sharing among internal security forces is an issue that characterises the intelligence community in South Africa. This has been a problem from the start and still remains a problem. It can be attributed to the need-to-know principle when protecting sources and professional jealousy between departments.

After World War II, the focus of the intelligence structures moved back to the internal situation. In order to increase effectiveness and on recommendation of Sillitoe, the SAP Special Branch (in 1950s referred to as Security Branch) was established by the SAP Commissioner in 1947 (Africa, 2009:65; Geldenhuys, 1984:147; O'Brien, 2011:18). This structure's main role was the "preservation of internal security", focusing on political crimes (Africa, 2009:65; Geldenhuys, 1984:147; O'Brien, 2011:18). The Special Branch operated alongside the Detective Branch and Uniform Branch of the SAP. The Head of the Special Branch became the chief security and intelligence advisor to the Union government (O'Brien, 2011:18). This created problems in that it politicised the position and the power and control would be centred in the hands of one person.

One of the major political events in the early South African history was the 1948 elections. During this election Smuts and his United Party lost to the Afrikaner National Party of Dr D.F.

Malan, who immediately introduced apartheid. Smuts used the DMI, which was perceived as pro-Britain, to monitor and counter Afrikaner nationalists (O'Brien, 2011:19). For this reason, after Malan came to power, the DMI was marginalised and reduced to only six officers (O'Brien, 2011:19). Because of its pro-Afrikaner nationalist views, SAP security intelligence interests grew in the 1950s. The Security Branch was engaged in tactical activities to collect information on political opponents of apartheid (Africa, 2006:74). After 1948, South Africa was increasingly isolated because of its apartheid policy. In order to combat the isolation and negative propaganda, the South African government placed information officers abroad. These efforts were augmented in 1957 with the establishment of the South African Information Services to influence foreign opinion in favour of South Africa's foreign and domestic policies (Africa, 2009:65). The Information Services and the Security Branch formed the backbone of the apartheid regime. Hendrik van den Bergh became the head of the Security Branch in 1960 (Geldenhuys, 1984:147; O'Brien, 2011:19). This started a new era of intelligence in South Africa.

Information on how the intelligence structures operated during this time is not readily available. Information is mainly limited to the structures and how these structures were established. However, it is safe to assume that intelligence was focused on internal security and that intelligence collection took place through human source networks. During this time external security collection was not yet established and the Union had to rely on the British to share this information. The intelligence structures in the Union obtained technology from Britain. South Africa was still a British Colony and the need for intelligence from all British protectorates necessitated the sharing of technologies. These technologies included radios, telephones, faxes and interception outfits. The period after 1948 laid the basis for the development of the apartheid intelligence services. The main focus of these institutions was collection and actions against opponents of apartheid.

The period discussed in this section witnessed the establishment of formal intelligence structures. It is especially the founding of the Security Branch towards the end of this time that played a crucial role in future developments of intelligence in South Africa. With this discussion as basis, the next section focuses on the first 20 years of independence.

6.4 Developments during first twenty years of independence: The Republic of South Africa (1961–1980)

One of the major events in South Africa's political development is 31 May 1961, when the country gained independence and became the Republic of South Africa. This event also saw

South Africa's withdrawal from the Commonwealth and links to British intelligence. Even though apartheid started in 1948, independence in 1961 solidified this policy and actions intensified to keep the status quo in place.

In order to meet the objectives set by the government, a coordinated security and intelligence architecture was of utmost importance. The DMI (structure under the South African Defence Force created out of the UDF) was established in 1962 with the function of collection, interception and dissemination of military security intelligence, national strategic intelligence and CI functions (O'Brien, 2011:23). During this time, General Retief (Chief of DMI) made a proposal to Vorster[38] (then Minister of Justice) that the DMI should focus on both military and domestic intelligence. However, this proposal was rejected (O'Brien, 2011:23). The domestic intelligence responsibility remained the mandate of the SAPs through the Security Branch, which was the second security structure to play an important role in the maintenance of national security. The Security Branch was under the leadership of the infamous Hendrik van den Berg. In 1963, Vorster instructed Van den Bergh to create a structure under the Security Branch known as the Republican Intelligence (RI) (Geldenhuys, 1984:147; Henderson, 1995:55; O'Brien, 2011:24; Sanders, 2006:12; Swanepoel, 2007:27). RI was responsible for internal security. However, this organisation was not very successful because of failing relations with Britain and the growth of the newly established DMI. According to O'Brien (2011:24), the main problem facing the RI was the fact that it was modelled on the CIA. However, their mandate was the collection and analysis of internal security, which is more akin to the Federal Bureau of Investigation's and MI5's responsibilities. Furthermore, Van den Bergh's personality also posed problems as he was felt to be using the RI to further his own political ambitions (O'Brien, 2011:24).

As the rivalry between the Security Branch and the DMI intensified, it affected coordination, rendering intelligence within the Republic inadequate. In an effort to address the coordination and rivalry problems, the State Security Committee (SSC) was established in 1963 (Geldenhuys, 1984:28; O'Brien, 2011:23). The departments that were represented on this committee include the Foreign Ministry, Military Intelligence and the Security Police. However, this did not alleviate the problem due to the dominance of the Security Branch and the control Van den Bergh had within the Branch (Africa, 2009:65; O'Brien, 2011:23). In another effort to improve coordination, the SSC was replaced by the State Security Advisory Board in 1966 (Geldenhuys, 1984:28; O'Brien, 2011:23). The main aim of this body was to coordinate intelligence activities. Nonetheless, this also failed, because of the personality

[38] Balthazar Johannes Vorster was the 7th Prime Minster of South Africa from 1966–1978.

clashes among the Security Branch and DMI and the lack of the demarcation of specific mandates between the two organisations (O'Brien, 2011:23).

During the late 1960s there was a perception that the Republic's intelligence needs were not fully met by the intelligence structures. In order to address this problem, Verwoerd[39] ordered Van den Bergh (at the time the recently appointed SAP commissioner) in 1968 to create a separate intelligence agency, outside of the Security Branch, responsible for NI functions (O'Brien, 2011:23). At first this new intelligence agency was formed around the RI. However, before this new agency could take shape, Prime Minister Verwoerd was assassinated and Vorster (then Minister of Justice, with the SAP as one of its main responsibilities) became the new Prime Minister. This did not derail the new structure and on 13 May 1969 the BOSS was established after the cabinet agreed to the establishment of a centralised intelligence service in 1968 (Africa, 2009:66; Geldenhuys, 1984:35, 147; O'Brien, 2011:25).

Coordination among the intelligence structures remained a problem and rivalry affected intelligence products. This problem escalated to such an extent that in 1970, Vorster appointed the Potgieter Commission to "Inquire into certain intelligence aspects of state security" (O'Brien, 2011:28). The Commission resulted in the establishment of the State Security Council (SSC) in 1972 (O'Brien, 2011:29). The SSC reported directly to the cabinet and represented the operational centre of the government's security strategy. The Potgieter Commission also clarified the role of BOSS as the primary security agency of the Republic. According to the Security Intelligence and State Security Council Act (64 of 1972) (cited by O'Brien, 2011:29) the SSC was to "(a) advise the government with regard to (i) the formulation of national policy and strategy in relation to the security of the Republic, and the manner in which such policy or strategy shall be implemented and be executed; (ii) a policy to combat any particular threat to the security of the Republic; and (b) to determine intelligence priorities". The SSC comprised the Prime Minister, the ministers of Defence, Foreign Affairs, Justice, Police; the heads of the SADF and the SAP; secretaries for Security Intelligence, Foreign Affairs and Justice and others co-opted to participate in relevant matters (Geldenhuys, 1984:92; O'Brien, 2011:29–30).

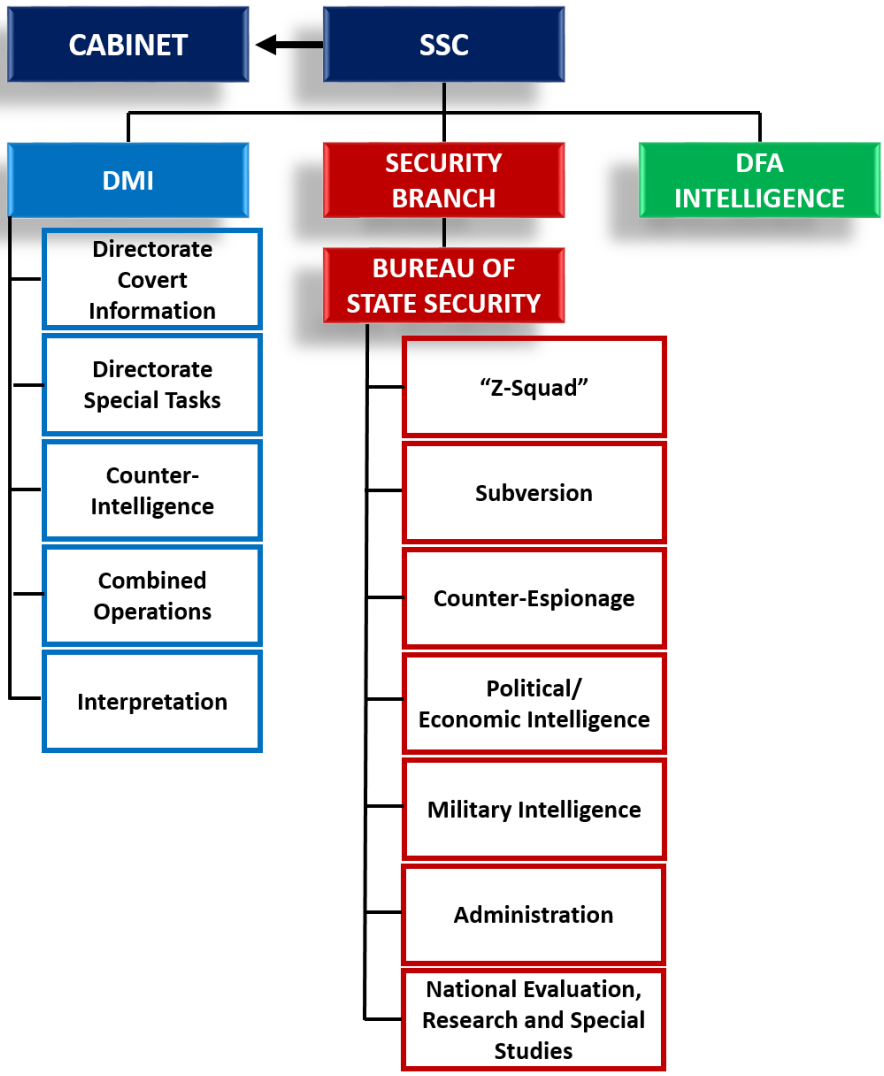
Although BOSS was established in terms of the Public Service Amendment Act (86 of 1969), this act did not give a full brief to the agency. The Security Intelligence and State Security Council Act (64 of 1972), however, laid out the purpose of BOSS in more detail (South

[39] Dr Hendrik Frensch Verwoerd was the leader of the National Party (NP) and the last Prime Minister of the Union of South Africa from 1958 to 1961. He continued as Prime Minister of the Republic of South Africa until 1966 (South African History Online, 2011).

African History Online, 2016a:1). The mandate of BOSS, according to the Security Intelligence and State Security Council Act (64 of 1972) (Africa, 2009:66; Geldenhuys, 1984:147), was the following:

- Collect, evaluate, correlate and interpret national security intelligence for the purpose of defining and identifying any threat or potential threat to the security of the Republic.
- Prepare and interpret (for the consideration of the State Security Council) estimates relating to any threat to the security of the Republic.
- Formulate a policy relating to national security intelligence for the approval of the state security council.
- Coordinate flow of intelligence between different government departments.
- Make recommendations to the state security council on intelligence priorities.

At this time BOSS served as the focal point for South Africa's intelligence activities domestically and abroad (Africa, 2009:67; O'Brien, 2011:26). According to O'Brien (2011:26), BOSS comprised six departments, which included Subversion, Counter-espionage, Political/Economic Intelligence, Military Intelligence, Administration and National Evaluation, and Research and Special Studies. Other structures included the Security Branch (SAP's) and DMI (Figure 43). The Security Branch was tasked with the responsibility of monitoring resistance through its networks of informants within anti-apartheid groups (Africa, 2009:67). The DMI produced intelligence on both internal and external role players in order for the SADF to plan military actions within South Africa as well as across South African borders. The position of Special Advisor on State Security was created under the Prime Minister and in October 1969, Van den Bergh was appointed in the position (O'Brien, 2011:25). Centralising the role in a person rather than a committee gave the Prime Minister more control over security issues in the country.



Source: Adapted from O'Brien, 2011:27

Figure 43: National Intelligence structure (1969–1978)

Another major political event that had far-reaching implications for intelligence in South Africa was the "Information scandal" of 1977–1978 (Geldenhuys, 1984:36; O'Brien, 2011:45). The "Information scandal" is also referred to as "Muldergate" after Dr Connie Mulder (Minister of Information), who was the main role player in this incident and was named as the person responsible for the irregularities in his department. The apartheid government attempted to influence political opinion abroad and locally by using official funds to purchase the Washington Star and establish the Citizen (Geldenhuys, 1984:36; O'Brien, 2011:45). The scandal also ended the political careers of Prime Minister John Vorster, Dr Nico Diedericks (Minister of Finance), Van den Bergh (Head of BOSS) and Dr Eschel Rhoodie (Secretary of Information) (Geldenhuys, 1984:36; O'Brien, 2011:45). Furthermore, the information scandal also affected the intelligence community as a result of the change in

leadership. Whereas Vorster preferred BOSS, PW Botha as the new Prime Minister (appointed on 28 September 1978) and previous Minister of Defence, favoured the DMI. Consequently, the DMI took over as the prominent role player with regard to intelligence and security matters (O'Brien, 2011:45).

During his first few years in office, Botha made a number of changes to strengthen the role of intelligence structures in terms of national security. An important change was the establishment of a new intelligence service (O'Brien, 2011:66). Various events led to the realisation that a non-military, non-police agency with a wider worldview was needed to provide strategic intelligence (O'Brien, 2011:66). These events and issues included the continued rivalry between the DMI and BOSS, the Information scandal and the failure of the intelligence community to predict the coup in Portugal in 1974[40], which led to the subsequent changed political landscape in both Angola (independence 1974) and Mozambique (independence 1975) (O'Brien, 2011:66). One solution was to mandate the Department of Foreign Affairs to provide strategic intelligence. However, this was difficult as the Department only had overt collection capabilities. In August 1978, Botha established the Department of National Security (DONS) (Geldenhuys, 1984:149; O'Brien, 2011:66; Sanders, 2006:108), which was based on principles of academic analysis to assist with strategic intelligence (in 1980 DONS was changed to the NIS).

In addition, a Working Committee was established, which was attached to the SSC (Geldenhuys, 1984:91-92; O'Brien, 2011:32). The main purpose of the Working Committee was to ensure the provision of coordinated intelligence to the security management system. The work of the SSC grew and by the end of the 1970s it had four branches:

- Strategic Planning Branch that was tasked with overseeing the national strategy of the government;
- National Intelligence Interpretation Branch (NIIB) that was responsible for the collation of intelligence products with information received from all the relevant role players;
- Administration Branch that was responsible for the Secretariat; and
- Strategic Communications Branch (Stratcom) that was the link between the SSC and various covert units (O'Brien, 2011:32).

The final and perhaps the most important change by Botha was the establishment of the National Security Management System (NSMS) in 1979 (Geldenhuys, 1984:93; Henderson,

[40] The Carnation Revolution started as a military coup and resulted in the authoritarian regime of Estado Novo being overthrown and the withdrawal of Portugal from its African colonies.

1995:53; O'Brien, 2011:84; Van der Waag, 2015:253). This new structure not only worked alongside the SSC, but also assisted the SSC. The NSMS was established in response to the *1975 Report on the National Security Situation,* which outlined a need for "an active security management system to link national, interdepartmental, departmental and the sub-departmental levels of operations" (O'Brien, 2011:84; Van der Waag, 2015:253). The main aim of the NSMS was to implement the "Total National Strategy". This strategy was devised by Botha, as he was of the opinion that there was a total onslaught[41] against South Africa from both inside and outside the country. Joint management centres (JMCs) were established that reported to the National Joint Management Centre under the SSC. These centres were divided internally (within South Africa) and externally, within the region. The internal centres were located at SANDF regional headquarters to oversee national issues, while the regional centres were established to oversee activities in countries such as Namibia, Angola and the Frontline States (Geldenhuys, 1984:93; O'Brien, 2011:86). All the security structures were focused on Botha's strategy. The goal of the strategy was to win support from western governments and to justify the cross-border raids on ANC camps in neighbouring countries.

The main focus of the intelligence community during this time was to secure the country against communism and in doing so, maintaining the apartheid regime. All resources and efforts were aimed at these priorities. In order to focus on these priorities, the intelligence community needed actionable intelligence regarding planned actions by anti-apartheid groups. Collection of information was done on two levels, HUMINT and SIGINT. Human source networks were established within the anti-apartheid structures to obtain intelligence. In addition to the human source networks, technology was also used to obtain and transmit information. These technology sources were aimed at interceptions of conversations between targeted members of the enemy of the state. The main role player for a great part of this period was BOSS. However, this situation changed when Botha became Prime Minister. Due to his background in the Department of Defence, the DMI became the intelligence structure of choice. This resonated with Botha's total onslaught paradigm and he used the military to counter internal and external threats within and outside of the country.

The first 20 years of apartheid consolidated the position of intelligence structures within the South African government. What is noticeable is that the preferred intelligence organisation changed with the changes in government leadership. This tendency continued throughout the next phase of apartheid and is discussed in the following section.

[41] Total onslaught refers to the threat against South Africa that was perceived on every level: political, economic, diplomatic, military, social and cultural (Van der Waag, 2015:251).

6.5 Developments from 1980–1994: The fall of apartheid

During this period, three intelligence capabilities served the government. The most important of the structures was DMI. Botha viewed the DMI at the centre of the security architecture and for this reason the DMI was tasked with the strategic intelligence brief. The DMI viewed everything through the lens of counter-revolutionary warfare (O'Brien, 2011:68). According to James Adams (cited by O'Brien, 2011:69), the DMI was guilty of creating "an intelligence picture which drove policy, rather than a policy which dictated the intelligence requirements". The intelligence focus during the early 1980s was driven by the DMI and the emphasis was on fighting the perceived communism threat and not even considering a negotiated settlement with the enemies of the state. DMI was the main role player under Botha and was responsible for the strategic intelligence brief, foreign intelligence collection and the domestic CI function. The second structure was the NIS. As indicated in the previous section, the DONS was changed to the NIS in June 1980 (Van der Waag, 2015:149; O'Brien, 2011:66; Geldenhuys, 1984:149). Botha appointed Dr Barnard as the Director General of NIS in 1980 with the brief to establish an independent intelligence organisation capable of providing long-term intelligence analysis to the Prime Minister (O'Brien, 2011:66; Van der Waag, 2015:149). Dr Barnard's vision was based on the methodology of the CIA, interacting with academics and implementing a more academic methodology within the NIS. The NIS had limited collection capabilities abroad, but was not mandated to collect intelligence within the borders of the country. Furthermore, it played an important role in the National Management Centre and the regional JMCs. The third structure was the Security Branch, which enhanced foreign intelligence collection (O'Brien, 2011:66).

During the 1980s two distinct views came to the fore (Barnard, 2015:30–31). On the one hand, the DMI and Special Branch were of the opinion that communism was the biggest threat to the Republic and that this problem could only be addressed with the use of force. On the other hand, the NIS was of the opinion that a negotiated settlement between the apartheid government and the ANC and its allies was the answer to the problems in the country. With this liberal political view and taking Botha's total onslaught paradigm into account, it is surprising that the NIS was not changed or even closed down. According to O'Brien (2011:71), the reason why the NIS survived during its early years was the fact that it was created by Botha himself.

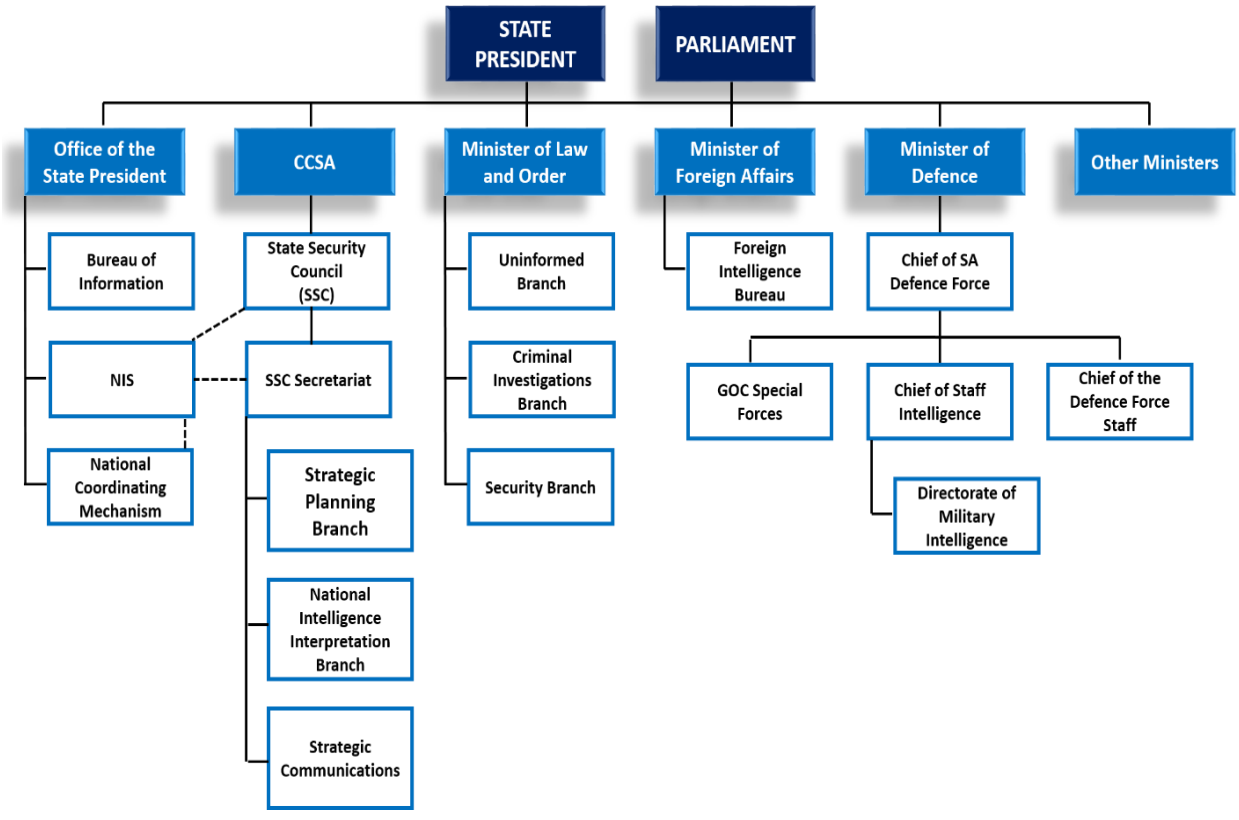
Coordination with regard to intelligence issues continued to pose problems for government. In 1980 Botha instructed the intelligence structures to be streamlined to address the in-

fighting and to ensure better coordination. In January 1981 a Rationalisation Committee was set up and they met in Simon's Town to deal with the instruction from the Prime Minister (Barnard, 2015:35–36; O'Brien, 2011:71). The outcome of the meetings was known as the Simon's Town Accords and included the following decisions:

- The NIS would be responsible for political intelligence, economic intelligence, counter-espionage and evaluation. The NIS had no offensive capabilities.
- The DMI would be responsible for military intelligence and contra-mobilisation and the handling of sources in other Frontline States and abroad.
- The Security Branch was responsible for domestic and international counter-subversion. The activities would also include dealings with sources in South Africa, Swaziland and abroad.
- In order to address the coordination issue Botha approved the National Intelligence Interpretation Branch (NIIB) and the Coordinating Intelligence Committee (chaired by Barnard) under the SSC Secretariat. Both the structures were approved in 1981. The main aim of the Coordinating Intelligence Committee was the closer coordination of the three main intelligence structures and other non-security structures such as the Department of Foreign Affairs. Various sub-committees supported the activities of the Coordinating Intelligence Committee. These included the Counter-revolutionary Information Task Team (Trewits – *Teen Rewolusionêre Inligting Taakspan*), Covert Information Gathering, Open Information Gathering, Technical, Evaluation, Counter-espionage and Security Intelligence (Barnard, 2015:35–36; O'Brien, 2011:71).

One of the important political events of the 1980s was the 1983 Constitution, which was led by Prime Minister Botha. This was South Africa's third constitution and replaced the republican constitution of 1961. Some of the most important changes were the establishment of the Tri-cameral Parliament permitting Coloured and Indian races to be represented in parliament on a segregational basis (South Africa, 1983:26). The second important change contained in the constitution was abolishment of the office of the Prime Minister to replace it with an executive state president, of which the first was PW Botha (South Africa, 1983:26). This position gave him much more power than the position of Prime Minister. The new state president had sole jurisdiction over matters of national concern, such as foreign policy, race relations and security issues. Furthermore, he increased his power over the security structures in the country.

Botha resigned as leader of the NP in January 1989 after suffering a mild stroke. In March 1989 the NP- elected FW De Klerk as the new leader of the NP and as state president. However, Botha first refused to step down and only resigned in August 1989. De Klerk was the seventh and last president of the apartheid government, appointed in August 1989. This was also the beginning of the end of apartheid, as De Klerk was in favour of a negotiated settlement. De Klerk inherited the securocrats from the Botha administration as part of the intelligence organisations, especially the SAPS and DMI. In order to move away from the securocratic government style, De Klerk made some changes to the security and intelligence community (see Figure 44). He moved the NIS (secret intelligence coordination) and the Bureau of Information (BI – responsible for overt government media activities) under his direct control so that they reported directly to the president (Henderson, 1995:55). The power of DMI was limited to addressing covert operations and the Security Branch was restructured into the Crime Combating and Investigation Service. During this time the NIS came to the fore as the prominent intelligence agency in South Africa with positive implications for the negotiation process.



Source: Adapted from Henderson, 1995:64

Figure 44: South African Security and Intelligence Community (1991)

He furthermore instituted an internal review process into the security architecture by the SSC Working Group (Henderson, 1995:55; O'Brien, 2011:178). This review resulted in various structural changes to address the securocrats' power over policymaking. The first step was the disbanding of both the NSMS and the SSC in 1991. The NSMS was replaced by the National Coordinating Mechanism and the SSC by the National Security Committee (NSC) (O'Brien, 2011:178; Henderson, 1995:58). The National Security Committee later became the Coordinating Intelligence Committee and in 1994 the National Intelligence Coordinating Committee (NICOC), which served under the newly established Cabinet Committee for Security Affairs (After 1994 it became the Cabinet Committee on Security and Intelligence – CCSI) (Henderson, 1995:58; O'Brien, 2011:178). This was an important move as the decision making now resorted with the Cabinet once again, unlike Botha's rule when these decisions resorted with the SSC (Henderson, 1995:58; O'Brien, 2011:178). This implied a broader scope of decision making and increased transparency. Secondly, the scope and mandate of the various intelligence organisations were addressed. In 1991 the Security Branch was combined with the Criminal Investigation Division into a new Crime Combating and Investigation Unit (Henderson, 1995:61). The NIS was responsible for the coordination of national strategic assessments for the state president and the Cabinet Committee for Security Affairs, and liaison with friendly intelligence agencies abroad (Henderson, 1995:61).

In February 1990, De Klerk unbanned the ANC, the South African Communist Party and the Pan Africanist Congress and Nelson Mandela and other political prisoners were released. Following these events, the ANC suspended their armed struggle on 7 August 1990. De Klerk's goal was a new political dispensation. To achieve this goal, he needed reliable intelligence. However, he had to deal with various issues or stumbling blocks and he needed information to assist with the transition process (Henderson, 1995:62). The information that was needed included intentions, planning, funding and support pertaining to various black opposition groupings within South Africa, white extremists, foreign countries and foreign organisations.

De Klerk made constant changes to his cabinet to reach his goal of a negotiated settlement. Roelf Meyer was appointed in 1990 as the Deputy Minister of Information Services in the President's office together with his position in Constitutional Development (Henderson, 1995:68). According to Henderson (1995:68), this was a strategic move, as he was of the opinion that De Klerk expected Meyer to shape the NIS into an organisation that would assist the president in his goals by providing negotiation intelligence. In the cabinet reshuffle of 1991, Roelf Meyer was appointed as Minister of Defence and the communication portfolio was also moved under his management (Henderson, 1995:70). In 1992 the Deputy Minister

of Finance (Theo Alant) was given a second responsibility, Deputy Minister of NISs, to perform a watchdog function over the covert operations (Henderson, 1995:70). This arrangement lasted until the next cabinet reshuffle in 1993 when the NIS was moved back to the Office of the State President with Justice Minister Coetzee responsible for its day-to-day management.

The NIS played a crucial role in the negotiated settlement. The first meeting between the intelligence organisations took place in September 1989 between members of the ANC's Department of Intelligence and Security (DIS) and the NIS (Barnard, 2015:198; O'Brien, 2011:1). However, the process was initially started in May 1988 when Barnard met Nelson Mandela for the first time (Barnard, 2015:198). This meeting started the process of transition and regular meetings between the intelligence services (NIS and DIS) took place to keep the process on track.

The timeframe was a crucial era in the political and intelligence history of South Africa. During this time the negotiation process for a more inclusive dispensation commenced and the NIS (civilian intelligence service) played a crucial role in realising this important political milestone. The focus of intelligence during this period can be divided into two phases. The first during the Botha era was focused on information pertaining to the anti-apartheid structures' plans with regard to actions against the government. During this phase the intelligence structures within defence and the police played an important role. The second phase, during the De Klerk era, was more focused on the negotiation process between the South African government and the ANC and its allies. The NIS played a crucial role. Information during this timeframe was obtained through human source networks and through the use of SIGINT. Furthermore, the computer and internet also played a critical role in obtaining overt information (OSINT) and served as a vital communication tool.

The ANC's intelligence arm played a crucial role in the transition process and the fall of apartheid and it is therefore important to discuss its history and development. The next section addresses these issues in more detail.

6.6 ANC intelligence

The ANC intelligence apparatus (DIS) is one of the main role players in the new intelligence structures and it is therefore important to examine this organisation in more detail. The ANC has existed since 1912, but its initial confrontation with the apartheid government of South Africa was based on peaceful mass actions. The decision to take up the armed struggle

came during the late 1950s when the ANC recognised that passive resistance and non-violence was not producing results (Department of Justice, 1996:26). The armed wing of the ANC/South African Communist Party was called *Umkhonto weSizwe* (MK – Spear of the Nation) and was established on 16 December 1961 with the main aim of waging a guerrilla war against the apartheid government in South Africa (Department of Justice, 1996:26; Williams, 2000:5). The chief objective was to overthrow the apartheid government to achieve democracy, freedom, peace and a country free of racism. The initial brief was to attack without the loss of life. Various senior commanders within MK were sent abroad for military training. MK followed the outline of guerrilla warfare with the following four phases: the original phase of the armed struggle was characterised by sabotage activities (lasting for more than a year), guerrilla warfare, insurrection and revolution (Williams, 2000:5). In the beginning the members lacked specialised training in covert operations. The South African government reacted with new laws in an attempt to address the sabotage activities. These included the General Laws Amendment (Sabotage) Act (76 of 1962), which allowed indefinite detention without a trial and the Unlawful Organisations Act (34 of 1960) that banned specified organisations. In reaction to these laws, the ANC established a mission abroad to mobilise international support and to secure training facilities for MK.

MK faced its biggest challenge in 1963 when the MK High Command was exposed, arrested and detained (Department of Justice, 1996:87). During the Rivonia Trial, the members were sentenced to lengthy periods of imprisonment. This forced the ANC and MK in particular to move abroad and establish training camps in countries such as Tanzania, Algeria and the former Soviet Union.

During the ANC's Morogoro Conference[42] (1969) in Tanzania, the Revolutionary Council was formed with the purpose of integrating political and military activities and to improve training of military personnel (Department of Justice, 1996:89; O'Brien, 2011:77). In 1969, the ANC's DIS (civilian intelligence arm) was formed after the conference to protect the organisation's human and material resources under Moses Mabhida (Department of Justice, 1997:59; O'Brien, 2011:78). This department was mandated with the following functions:

- Prevent infiltration by members of the apartheid government's security forces;
- Gather information about the apartheid government's strategies and intentions;
- Minimise damage due to infiltration by apartheid forces; and
- Assist with reconnaissance of targets in South Africa to develop in potential operations.

[42] The ANC's first National Consultative Conference was held in Morogoro in 1969.

By 1981 the ANC National Executive Committee appointed a National Directorate of DIS with three main sectors: intelligence, security and processing of information (Department of Justice, 1996:148). In July 1987 DIS was restructured to form the Department of National Intelligence and Security (NAT), with intelligence, CI, processing and security sub-sectors (Department of Justice, 1996:148; O'Brien, 2011:173). The MK activities can be divided into the following timeframes:

- From inception to 1969: Sabotage campaign – strategic roads, power stations, police stations, military camps and military forces.
- From 1969 to 1979: The focus shifted from sabotage to guerrilla warfare. Guerrilla operations focused on economic infrastructure, military targets, and political state infrastructure.
- Guerrilla warfare and people's war 1979–1990: The armed activities went with an organised underground political presence.
- Post-1990: Suspension of the armed conflict (Department of Justice, 1996:91).

Military activities remained at a low level during the 1960s and the early 1970s. However, various factors played a role to improve the operational circumstances of MK from the mid-1970s. These included the following:

- Release of some of the MK commanders captured previously.
- Independence of Mozambique and Angola.
- The 1976 student uprising.
- New training camps in Angola.
- From 1977 a large number of fighters made their way back into South Africa (Williams, 2000:8).

ANC activities became more sophisticated and increased in regularity from 1977. Successful hits include the Sasol oil refinery (1980), Koeberg (1982), the South African Air Force and the Military Intelligence Offices (1983) (Department of Justice, 1996:10; Williams, 2000:9–13). In spite of the mentioned successes, the armed struggle did not have the impact the members had hoped for (Jenkin, 1995). After some examination, the conclusion was reached that one of the key problems facing the organisation was the lack of communication between the leadership abroad and the membership in South Africa (Garrett & Edwards, 2007:4; Jenkin, 1995). It was not until Operation Vulindlela (Vula) that the communication was more successful (Jenkin, 1995:4). During the early 1980s the ANC founded the ANC

Technical Committee to provide technical support to the struggle and to assist with communications between members inside the country and the leadership abroad (Garrett & Edwards, 2007:4). In 1986, MK initiated Operation Vula. It involved the deployment of senior and middle-ranking MK members in exile back to South Africa to develop underground structures within South Africa (Department of Justice, 1996:23; Department of Justice, 1997:15; Williams, 2000:13–15). The Technical Committee was tasked with the communications for Operation Vula. During this time the Committee developed an encrypted communication system by using commercially available computer equipment, computer encryption programmes and international telephone systems (Garrett & Edwards, 2007:4; Jenkin, 1995:5). The ANC also used old acoustic modem/tape recorder systems and pager- and voicemail (Jenkin, 1995:3). The operation successfully infiltrated the NIS and Special Branch and smuggled weapons into the country. The unbanning of the ANC in 1990 brought a ceasefire between MK and the security forces and the end of Operation Vula.

The actions of the ANC played a crucial role in the democratic change in South Africa. Through the use of technology such as computers, encryption programmes and telephones, the ANC improved communication between the leadership and the members, increasing the organisation's capacity to affect change.

These advancements described above played a vital role in the move to democracy. This serves as an introduction to the final period of intelligence progress after the 1994 elections.

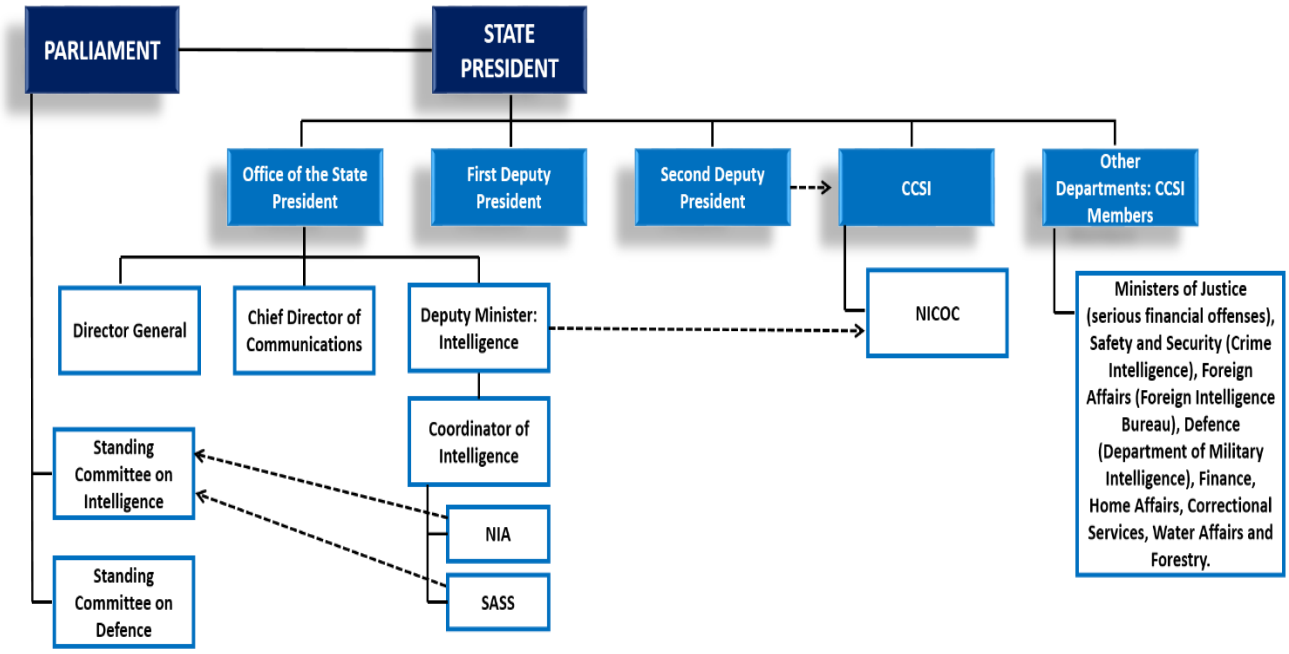
6.7 Developments after the democratisation of South Africa (1994–present)

Although various milestones can be identified in the South African political history, the most significant political event was the first democratic general elections that took place on 27 April 1994. As throughout history, this event also had an impact on the development of the intelligence community. Since the election in 1994, the development of the intelligence services can be divided into three phases (Africa, 2009:97–98).

6.7.1 First phase

The first phase started in 1994 under the presidency of Nelson Mandela. The intelligence architecture of 1994 was faced with a major problem of fragmentation. Various intelligence organisations had to be integrated into one organisation. These intelligence organisations

included the NIS, the ANC-DIS, the Pan Africanist Security Service (PASS), homeland[43] intelligence organisations (Transkei Intelligence Service – TIS, Bophuthatswana Internal Intelligence Service – BIIS and Venda NIS – VNIS) and other intelligence organisations attached to political organisations (Africa, 2009:75; O'Brien, 2011:208; Africa, 2012:107). This integration took place in accordance with the Transitional Executive Council Act (151 of 1993), Section 20. According to the Act, a Sub-Council on Intelligence was established with the main focus of political supervision and oversight over the statutory and non-statutory intelligence structures (South Africa, 1993:28–30). Deputy President FW De Klerk was appointed as the chairperson of the CCSI (Africa, 2012:104; Henderson, 1995:474; O'Brien 2011:212). Within the new cabinet, a new intelligence portfolio was created, namely the Deputy Minister of Intelligence Services under the Office of the State President (Henderson, 1995:478; O'Brien 2011:205). Even though the day-to-day activities were taken care of by the CCSI, this new portfolio provided the State President with control over the civilian intelligence services.



Source: Adapted from Henderson, 1995:472

Figure 45: South African Security and Intelligence Community (January 1995)

The establishment of the new intelligence services took place on 1 January 1995 when the NIS was terminated and the new National Intelligence Agency (NIA) with a domestic security intelligence focus and the South African Secret Service (SASS) with a foreign intelligence

[43] The apartheid government established demarcated homelands to which the Black population was moved to prevent them from living in the urban areas of South Africa (South African History, 2011).

focus were established in terms of the National Strategic Intelligence Act (39 of 1994) (South Africa, 1994b:4). The new NIA and SASS comprised all the former intelligence services[44] (Africa, 2012:107; Africa, 2009:75; O'Brien 2011:208). The Intelligence Portfolio (as depicted in Figure 45) reported to the Deputy Minister of Intelligence Services, who in turn reported to the Minister of Justice and the Office of the State President (O'Brien, 2011:205). The NIA was mandated to focus on domestic security issues, while SASS was responsible for collection of information with regard to foreign threats and to liaise with foreign intelligence partners (South Africa, 1994b:4).

During the early stages of the democracy, various policy documents and legislation played a crucial role with regard to the establishment and activities of the intelligence structures. These acts were introduced towards the end of 1994 and focused on mechanisms for control, coordination, oversight and accountability with regard to the intelligence community.

The first policy change pertaining to the establishment of the new civilian intelligence structure is the White Paper on Intelligence, which provided the framework for intelligence within a democratic society. Some of the key issues addressed included that domestic political opposition was no longer the primary threat, use of intrusive collection was only allowed in certain situations and the defence force was no longer involved in domestic intelligence collection (South Africa, 1995:1–12). These issues were key in the apartheid intelligence dispensation and to create an intelligence service that was in line with a democratic South Africa, it was important to address these matters. The White Paper also contains a section "code of conduct", which plays an important role in oversight and control.

The second important change was the National Strategic Intelligence Act (39 of 1994), which established a NICOC and provided for the appointment of the chairperson of the National Intelligence Co-ordinating Committee (South Africa, 1994b:9). According to the Act (South Africa, 1994b:9), NICOC was tasked with the integration of input from the NI structures (NIA, SASS, intelligence division of the SAPS and the SANDF). The coordinator was tasked to manage and administer the NICOC process (South Africa, 1994b:9). NICOC was responsible for overseeing the coordination of the intelligence services, to monitor if all representatives where working according to their mandate, and reporting to the president through the CCSI. NICOC was furthermore responsible for the coordination of the NIE on a yearly basis with input from all relevant departments. The NIE formed the basis of the NI

[44] The intelligence services included the NIS, the ANC-DIS, and the intelligence services from the previous Transkei, Bophuthatswana and Venda, the Pan Africanist Congress Security Services and intelligence members attached to any political party.

priorities, which were disseminated to all relevant departments as a basis for operations for that year. NICOC comprised the NI coordinator, the director general of each service, the head of crime intelligence and DI. Sharing of information was addressed in memoranda of understanding between the various intelligence structures. This together with the mandates addressed the issue of competition between the structures. The heads of the various security services (NIA, SASS, Defence Intelligence of the SANDF, Crime Intelligence of the SAPS and Department of Foreign Affairs later) had to meet on a regular basis under the National Intelligence Coordinator.

The next important change is the Intelligence Services Oversight Act (40 of 1994) that dealt with oversight. This act made provision for the establishment and functions of a committee of members of parliament on intelligence (Joint Standing Committee on Intelligence) (South Africa, 1994a:4; Africa, 2009:84; Dlomo, 2004:57; O'Brien 2011:214) and the appointment of the Inspector General of Intelligence (South Africa, 1994a:11). Some of the main functions of the Inspector General are to "monitor compliance by any Service with the Constitution, applicable laws and relevant policies on intelligence and counter intelligence" and to "review the intelligence activities of any Service" (South Africa, 1994a:11). The Inspector General is accountable to the Joint Standing Committee on Intelligence, which reports directly to the president. It is a parliamentary oversight body with representatives from the largest political parties.

The fourth important document with regard to the intelligence services is the new Constitution, which outlines the role and mandate of the intelligence and security services (Section 185 of the Constitution of South Africa). The Constitution protects against state abuse of power and is also a mechanism for oversight.

With regard to the other national security structures, the South African Police Service Act (68 of 1995), the National Crime Prevention Strategy of 1996 and the White Paper on Defence: Defence within a Democracy 1995 are relevant (O'Brien, 2011:210). In July 1994, the Crime Combating and Investigation Unit of the SAP was disbanded and replaced by the National Crime Investigation Service (O'Brien, 2011:210). Within the SANDF, the DMI was replaced by an intelligence division (ID) with the mandate to provide foreknowledge of military threats and strategic military intelligence (South Africa, 2002a:36; O'Brien, 2011:210). Oversight for these divisions is provided for through the Parliamentary Joint Standing Committee on Defence and Intelligence, the Inspector General of the SANDF and Intelligence and NICOC (O'Brien 2011:211).

6.7.2 Second phase

The second phase of intelligence changes took place during President Mbeki's term. These changes were aimed at expanding intelligence structures and strengthening institutional culture (Africa, 2012:109). An important change in the administration and control of the civilian intelligence services took place in 1999 when President Mbeki changed the portfolio from Deputy Minister to Minister of Intelligence (Africa, 2012:111).

Together with above-mentioned change, various acts were introduced. The first was the Promotion of Access to Information Act (2 of 2000). This act was aimed at improving information security in government (South Africa, 2000:1). The second important act was the Intelligence Services Act (65 of 2002), which replaced the Intelligence Services Act (38 of 1994) that was repealed in 2002. The Act reconfirmed the NIA and SASS and established a South African Academy of Intelligence and a Ministerial Advisory Committee on Training (South Africa, 2002c:1). The aim of the Academy was to provide training for intelligence officers and cadets of the civilian intelligence services. Furthermore, the Act called for the establishment of an Intelligence Services Council on Conditions of Service, which had to make recommendations to the minister with regard to conditions of services and human resource issues (South Africa, 2002c:1).

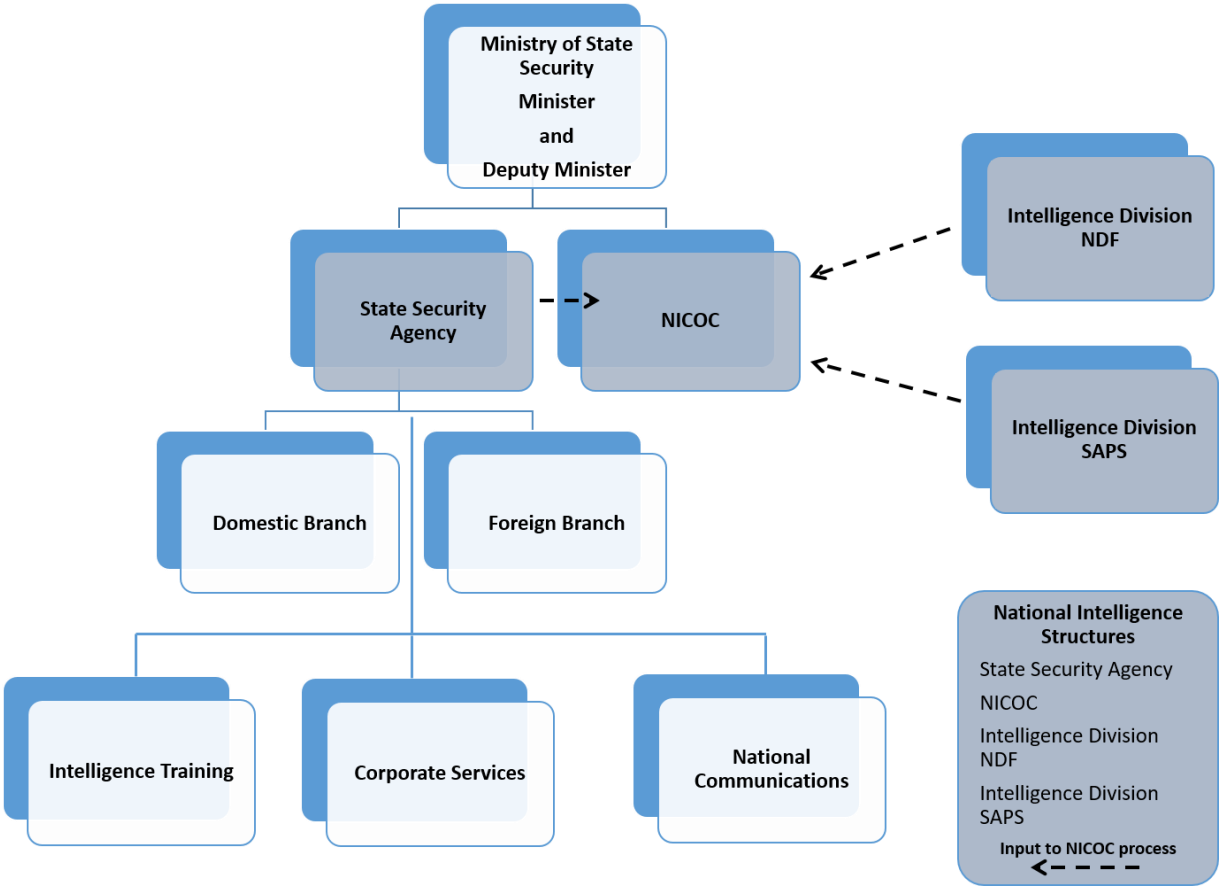
Three developments during this timeframe played a crucial role with regard to technology development within the intelligence service. The first one was the Electronic Communication Security (Pty) Ltd Act (68 of 2002) (South Africa, 2002b) which established COMSEC (Electronic Communications Security). The main functions of COMSEC were to:

- protect and secure critical electronic communications against unauthorised access, or technical, electronic or any related threats;
- provide a verification service that concurs with the NIA for electronic communications security systems, products and services used by organs of the state;
- provide and coordinate research and development with regard to electronic communications security systems, products, services and any other related services; and to
- perform any other services not inconsistent with the Act necessary for the effective functioning of COMSEC (South Africa, 2002b:4).

The second important piece of legislation was the Regulation of Interception of Communications and Provision of Communications-related Information Act (70 of 2002), also referred to as RICA. This Act was amended in 2004 and in 2010. Section 33 of this Act established the Office for Interception Centres (OIC) and with the necessary warrant it is the only structure with the authority to engage in the legal interception of domestic communications (South Africa, 2002d:64).

The third and final development was the establishment of the National Communication Centre (NCC). The NCC was established by the Intelligence Services Amendment Bill of 2008 where section 3(2) A of the Intelligence Services Act (65 of 2002) was amended to include the establishment of the NCC (South Africa, 2008:3). The NCC deals with foreign signal interceptions in South Africa. While RICA governs domestic communication signal interceptions, there is currently no law regulating the NCC or foreign signal interception in South Africa (Swart, 2016:3).

6.7.3 Third phase



Source: Adapted from SSA Ministry Website

Figure 46: Ministry of State Security (2013)

The third timeframe of the post-1994 intelligence dispensation started in 2009 when President Zuma became president. The State Security Agency (SSA) was formed in 2009 to incorporate the NIS, SASS, Intelligence Academy, NCC and COMSEC (South Africa, 2009a:3; South Africa, 2009:7; South Africa, 2009c:11; South Africa, 2009d:15). In 2009 the ministers of State Security, Police, Defence, Home Affairs, Justice and Correctional Services were tasked by the President to review the structures of the civilian intelligence community to develop a more effective and efficient structure. This process culminated in the General Intelligence Laws Amendment Act (11 of 2013) (South Africa, 2013). The outcomes with regard to the structures are depicted in Figure 46. The SSA, which was formed in 2009, was confirmed by law in 2013 (South Africa, 2013:20) and according to the Act, the NI structures comprises NICOC, the ID of the National Defence Force, the ID of the SAPS and the SSA (South Africa, 2013:6).

The intelligence development during this timeframe is characterised by continuous changes. The slow securitisation of the intelligence in South Africa is evident from the changes in the intelligence structure since 1994. The first cabinet of President Nelson Mandela did not have a Minister of Intelligence. However, in 1995, Joe Nhlanhla was appointed as Deputy Minister for Intelligence under Justice Minister Dullah Omar. In 1999, intelligence became a full cabinet portfolio under President Mbeki. This was followed by yet another change by President Zuma, who changed the portfolio from Intelligence Services to State Security, after which he appointed a Deputy Minister for State Security in his 2014 cabinet. The technology development during this timeframe followed the global developments. The main progress was expansion in the use of digital communication technology, specifically mobile phones, computers and internet.

These technology developments referred to briefly above are reviewed in the next part of this chapter.

6.8 Technology in the South African intelligence environment

The previous chapter explained in great detail how technological development contributed to the evolution of global intelligence. In South Africa a limited amount of information is available with regard to technology development within the intelligence services. Technology within the intelligence services is of a highly sensitive and secret nature because of the way in which information is accessed and the nature of the information itself. Intelligence services are not keen on sharing their technological capabilities because of the secret environment of these organisations. The American National Security Agency and British Government

Communications Headquarters do not share their capabilities. The American National Security Agency's capabilities have only recently come to the fore when Edward Snowden leaked classified information.

With regard to the South African context, technology development has taken place along the same lines as did the rest of the intelligence organisations around the globe. Table 6 illustrates intelligence sources, methods and priorities during various political periods in the history of South African politics. It also indicates the most important technologies used during that specific time

During the early stages of intelligence development in South Africa, encrypted radio, telephone and fax messages were used extensively for communication purposes. The intelligence organisations also had the capability to intercept communications from the mentioned equipment. From the early 1960s until the early 1990s, communication (radio and telephone) between anti-apartheid movements were intercepted by the apartheid government's security structures and used to counter planned actions (Mostert, 2017). Technology developments such as the internet and computers have increased since the end of the Cold War. However, one of the main tools of intelligence remains the interception capabilities of the NCC in Pretoria. Another source of information that has increased in importance and in volume is OSINT. This increase is linked to the information age of computers, internet and mobile phones. The technology development has increased access to and use of open source information in intelligence products. Another important result of the technology development has been social media platforms and information linked to these platforms. As indicated earlier, these platforms create enormous amounts of useful information (SOCMINT) that can assist intelligence organisations in compiling the national security picture. However, in the case of South Africa, SOCMINT is not yet recognised as a source of intelligence and is not included in the intelligence framework for collection purposes. The huge potential of SOCMINT makes it important to first understand the source of information fully and secondly to understand how to include it in the intelligence collection framework.

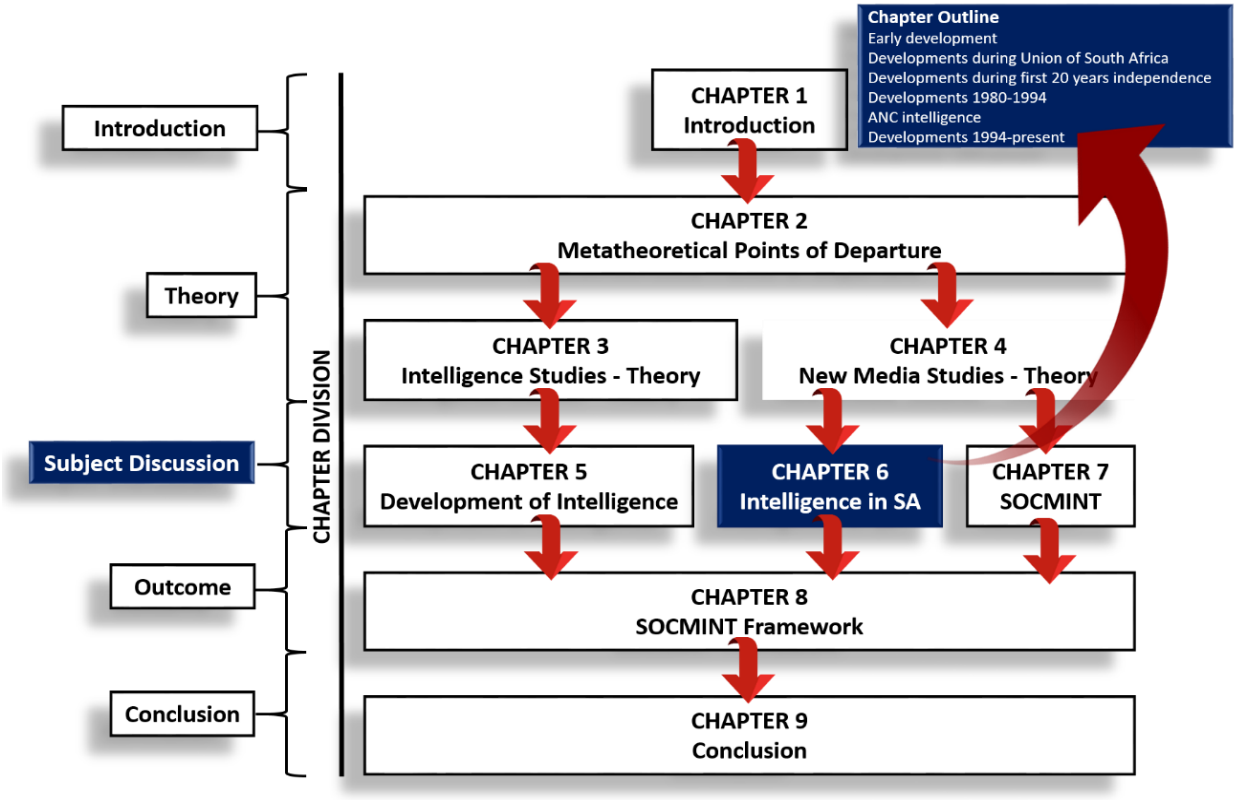
Table 6: Timeline: Intelligence and technology development

INTELLIGENCE	TIMEFRAME	TECHNOLOGY
Sources: HUMINT, Interceptions of radio messages and written messages **Method:** Messages sent in codes, ciphers to decode messages, agent networks, covert action – propaganda in European media **Intelligence priority:** Information regarding British forces, movements and plans	**Early development: Late 1800-1910**	Telephone and fax machines
Sources: HUMINT and SIGINT **Method:** Agent networks and interceptions **Intelligence priority:** Internal political situation	**Union: 1910-1961**	Radio, telephone and fax machines
Sources: SIGINT, HUMINT **Method:** Agent networks, interceptions **Intelligence priority:** Internal political situation, securing and maintaining the apartheid regime	**Republic: 1961-1980**	Radio, telephone, fax machines, computers
Sources: HUMINT, SIGINT, OSINT **Method:** Agent networks, Interceptions **Intelligence priority:** Until 1989 it was information to secure and maintain the apartheid regime, from 1989 information to assist the transition process	**1980-1994**	Radio, telephone and fax machines computers
Sources: HUMINT, SIGINT, OSINT **Method:** Agent networks, Interceptions **Intelligence priority:** National security of South Africa	**1994-Current**	Radio, telephone, computers, mobile phones and internet

Source: Adapted from Van Den Berg, 2014:18

6.9 Conclusion

The South African intelligence dispensation has always been in transition, especially since 1994. Prior to 1994 the security structure of choice was dependent on the prime minister and later president and his priorities. Vorster used BOSS and the police to reach his goals; Botha used DMI to interact outside of the country and De Klerk used NI to assist him with the transition process. After 1994 the intelligence services has been in a constant state of reform and restructuring.



Source: Own construct

Figure 47: Chapter Summary

Figure 47 provides a summary of the chapter outline and its position in the study. This chapter first explained the development of the South African intelligence services to understand how the current dispensation came about. This was followed by an overview of the technological development. Together with the development of the intelligence services and technology, the chapter also briefly referred to the sources of information used during each phase of development. South African intelligence primarily made use of HUMINT, SIGINT and OSINT. However, SOCMINT, which is an important source of information from

new technologies, is not yet included in the framework. The aim of this study is to compile a strategic framework to incorporate the new phenomenon of SOCMINT in the intelligence environment. It is essential to understand the development of the organisation to compile this framework and to shape SOCMINT as a source of information.

In order to compile the framework to include SOCMINT it is critical to also understand the phenomenon of social media. The next chapter focuses on what social media entails, how it is applied within the global communication environment and the application of SOCMINT within the intelligence environment.

CHAPTER 7: SOCMINT AND ITS GLOBAL APPLICATION

The fact that the Arab Spring protests were organised online suggested that traditional intelligence indicators were especially irrelevant. Now the best way to keep up with major political change was seemingly not through espionage but by paying close attention to new media.
J Rovner 2013

7.1 Introduction

After the end of the Cold War, political, economic and social boundaries diminished as a result of globalisation. The world has become a smaller place. This reality of a world without boundaries has been amplified by the digital revolution, especially the internet and its applications. Communication can now take place any time and from anywhere in the world. The digital technology is transforming social behaviour and society as a whole. Currently the internet is a space where information and thoughts are exchanged freely. Social activities are increasingly taking place in cyber space, which is a sphere that is not governed by a specific governing body and where rules and regulations are difficult to enforce. The current global landscape is characterised by social, technology and cultural change, which Lister *et al*. (2003:11) refer to as the "techno-culture".

The main goal of intelligence is to understand human behaviour and how it affects national security. One of the most fundamental needs of humans is to socialise and to communicate. Communication has been revolutionised over the past 20 years due to ICT developments such as the internet and social media. The new social media platforms have created new ways of communicating and interacting between people. This widespread use and access to the internet and wireless communications have increased people's awareness and access to information. This has also created new challenges for organisations with regard to the safeguarding of information and the public at large.

According to Wark (1993:2), the "intelligence revolution" has manifested in the 20th century and communication technology development has played a crucial role in raising intelligence organisations' profile and productivity. This revolution started during World War I and II with SIGINT and has continued to the phase of the computer and the internet. The age of the internet and the subsequent information explosion have increased the impact of technology on intelligence and the need to understand new communication technologies to safeguard national security. The new communication technology of social media has changed every aspect of our lives and has touched our social interaction and how we do business. It is only

realistic that it will also have implications for national security and the intelligence environment. In line with this development, the focus of this study is to create a framework to understand and include the intelligence generated from social media interactions (SOCMINT) in the intelligence environment. This chapter examines social media from an intelligence perspective to understand how the intelligence generated from social media can be applied within the intelligence environment. In order to reach this goal, the purpose of this chapter is the following:

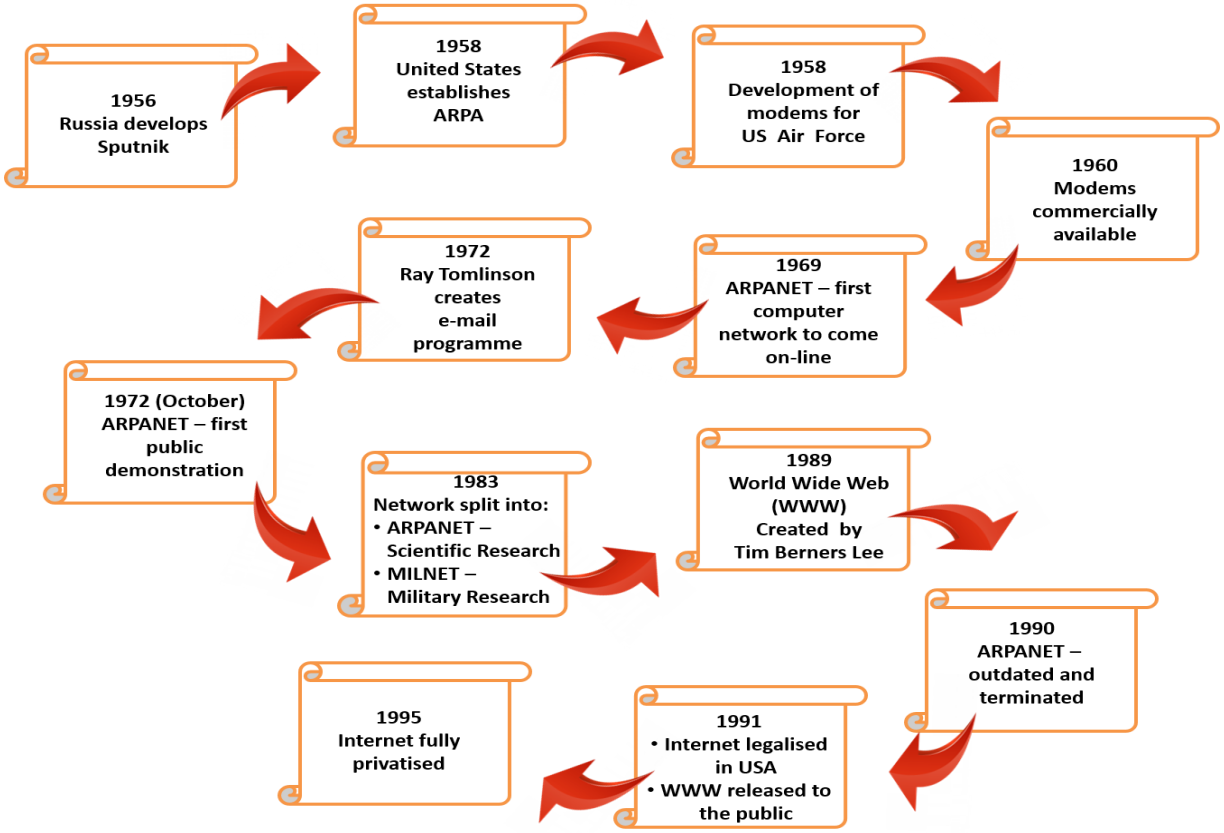
- The first section outlines the history and characteristics of the internet, which forms the basis for social media.
- The next section defines social media and explains its origin, functions, characteristics and applications.
- This discussion is followed by an in-depth analysis of the global digital landscape.
- The subsequent discussion focuses on the threats and opportunities of social media for national security.
- The final section of this chapter focuses on SOCMINT as a new source of intelligence collection, its application within the intelligence environment and understanding the challenges linked to this important source of intelligence. This section also includes case studies of social uprisings where social media played a crucial role.

The chapter begins with a brief history and characteristics of the internet. The internet forms the backbone of social media and it is therefore important to contextualise this technology development.

7.2 The history and characteristics of the internet

Before social media can be discussed in detail, it is important to first highlight the technology behind this phenomenon, the internet. Even though there have been great technology developments in the last century (see Chapter 5), the development of the internet can be viewed as one of the most important communication infrastructural expansions. This is true mainly because its impact is far-reaching and influences every aspect of our daily lives in terms of social interaction, conducting business, government relations and training and development. According to the Concise Oxford English Dictionary (2004:742), the internet is “a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols”. This definition is sufficient for the purposes of this study.

The history of the internet is explained in Figure 48. The internet has its origins in the USA as a result of developments in the previous USSR. It was the launch of the Sputnik in 1957 by the USSR that sparked the establishment of the Advanced Research Project Agency (ARPA)[45] in 1958 as part of the United States of America Defence Department (Abbate, 1999:36; Castells, 2010b:45; Hobbes, 2018:1; Keefer & Baiget, 2001:90). ARPA was tasked with the development of a communication system that could withstand a nuclear attack (Castells, 2010b:45; Hobbes, 2018:1; Keefer & Baiget, 2001:91). During the Cold War, the possibility of a nuclear attack was great, and it was important to the USA that communication systems were not compromised during such an attack.



Source: Own construct

Figure 48: Historical overview of the development of the internet and world wide web

An important device that played a crucial role in the development of the internet is the invention of modems. The modem (modulator-demodulator) is a device that enables communication between computers by converting digital signals into analogue signals and back (Internet Hall of Fame, 2016:1). Modems were developed in 1958 (Internet Hall of

[45] ARPA is a science and technology agency that was established during the Cold War and focused on military advancements (Abbate, 1999:36; Castells, 2010b:45).

Fame, 2016:1) to assist the United States Air Force to transmit data. Commercially they were only available by the early 1960s (Abbate, 1999:1). The outcome of the ARPA task was the ARPANET, the first computer network that went online in September 1969 (Castells, 2010b:49; Keefer & Baiget, 2001:91; Leiner *et al*., 2009:24). The ARPA communication system project was constructed around packet-switching[46] technology, which allowed for a network that was independent from command and control centres (Castells, 2010b:45; Keefer & Baiget, 2001:90).

Another important development was the creation of an e-mail programme by Ray Tomlinson in 1972 to send messages across a distributed network that he expanded to ARPANET users using the "@" sign as part of the address (Hobbes, 2018:4; Leiner *et al*., 2009:24; Internet Hall of Fame, 2016:1). The first public demonstration of the new network technology (ARPANET) was done in October 1972 at the International Computer Communication Conference (Abbate, 1999:79; Leiner *et al*., 2009:24). During the 1970s, access to ARPANET was dedicated to military and other scientific research (Castells, 2010b:50). However, with the increase in scientific use of the system the decision was taken in 1983 to split the system into the ARPANET (scientific research) and MILNET (military research) (Castells, 2010b:50). One more significant development in the history of the internet was the creation of the World Wide Web (www) by Tim Berners-Lee in 1989 (Donato, 2010:60; Internet Hall of Fame, 2016). According to the Concise Oxford English Dictionary (2004:1663), the World Wide Web is defined as "an extensive information system on the internet providing facilities for documents to be connected to other documents by hypertext links". It is important to note that the internet and the World Wide Web are not the same – the World Wide Web is a computer system that uses the internet to connect documents and pictures.

By 1990 the ARPANET technology became out-dated and was terminated (Castells, 2010b:50; Hobbes, 2018:11–12; Webopedia, 2007:1). The backbone of the internet was then taken over by the National Science Foundation, which was the last government-operated internet backbone (Abbate, 1999:199; Castells, 2010b:50). In 1991 the commercial use of the internet was legalised in the USA and the World Wide Web was launched to the

[46] Packet-switching is a method used to transmit data across a network. The message is broken down in packets that is transmitted individually across a digital network and then reassembled into the original message at the end destination (Abbate, 1999:7; Gorry, 2001:1). In 1961 the concept of packet-switching was established by Leonard Kleinrock at the Massachusetts Institute of Technology (Internet Hall of Fame, 2016:1).

public and the phrase "surfing the internet"[47] was coined in 1992 (Hobbes, 2018:11–13; Webopedia, 2007:1). In 1995 the internet was fully privatised (Abbate, 1999:199; Castells, 2010b:50).

With the history of the internet as background, it is imperative to highlight the characteristics of this technology. After studying the history of the internet it became clear that its characteristics can be divided into two categories: characteristics in relation to the technical aspects or architecture of the internet and characteristics pertaining to the application of the internet (Daigle, 2015:2; Hill, 2013:2; Internet Society, 2016:2). This study looks into the application characteristics as applicable to social media.

When examining the internet, a few characteristics are prominent and clearly relevant to social media. The first of these characteristics is its global nature (Daigle, 2015:5; Internet Society, 2016:2; Potts, 2014:3). According to Kemp (2018), more than 4 billion people around the globe have access to the internet, which is indicative of the globalised nature of this technology. Even though internet penetration is only 53% around the globe, there are very few countries in the world that do not have access to the internet. Only three countries (North Korea 0.06%, Eritrea 1% and Niger 4%) have less than 5% internet penetration (Kemp, 2018). The reasons for poor penetration include a lack of infrastructure, poverty and government regulations. It is this globalised characteristic of the internet that also plays a crucial role in social media. Social mobilisation and the distribution of information can reach a vast number of people from a single computer.

The second characteristic of the internet is that it allows for a two-way flow of communication without taking any borders into account (OECD, 2014:6; Potts, 2014:5). Another characteristic is its ease of accessibility (Hill, 2013:1; Potts, 2014:7). The cost of connection is low and with a computer or cell phone and internet connection, it is relatively easy to design and establish a website. This allows a user to distribute information globally and at a very low cost. Anonymity is an additional characteristic that allows users to post information and comments without the fear of being known (Potts, 2014:7). While it has created a society that is less inhibited, it has led to the problem of a lack of responsibility on the part of users with regard to comments and information posted.

One more characteristic is that the internet serves a general purpose (Daigle, 2015:5; Internet Society, 2016:1). Although the internet was developed from the ARPA brief

[47] To "surf the internet" implies to move from one website to another to research a topic of interest (Intel Corporation, 2015:1) by means of hypertext (see section 4.6).

explained above, it was not invented with a specific purpose in mind (Daigle, 2015:5; Internet Society, 2016:2). However, it ended up serving a wide variety of purposes such as business, teaching, communication and news. The networks within the internet, however, can focus on a specific issue (for example, Facebook® focuses on social interaction).

The last characteristic of the internet that is of importance to this study is the fact that this technology is perceived as borderless (Hill, 2013:11; Internet Society, 2013:1; Malcolm, 2013:3; Svantesson, 2006:4). Information can effortlessly and immediately be transferred across borders without taking country rules, regulations and laws into account.

With this brief explanation of the internet's history and its characteristics as background, the next section focuses on describing what social media entails.

7.3 Defining social media

Social interaction and communication have been taking place since the beginning of time and the sociable use of media in this interaction is not a new occurrence (Boyd, 2009:1). However, the current technology changes, such as the computer, internet and social networking sites, have fundamentally changed the way in which social interaction takes place. The current web-based application of social media is one of the most significant trends over the last 20 years. The pace of changes within society is directly linked to the pace of technological change. Bauman (2006:12) aptly describes the current society as "liquid", because society is always in a state of change. It is specifically social media that is contributing to major changes within the communication environment, impacting on the way people interact with each other. The phenomenon of social media started in 1997 with SixDegrees.com, which was a basic text-only network site, based on users entering e-mail addresses of relatives and friends and in doing so, growing the network (Brunty *et al*., 2013:2; Ryan, 2010:149). This has developed into a plethora of sites such as Facebook®, YouTube™, Twitter® and Instagram™.

Why is the popularity of this phenomenon of social media increasing at such a pace? One of the main reasons is that it addresses the important human need of social interaction (Leiter, 2014:1; Pirsig, 2012:10). As stated in the introduction, humans are social beings and according to Riva (cited by Montagnese, 2012:7) and Boyd *et al*. (2010:6), the following are some motivations behind the use of social media:

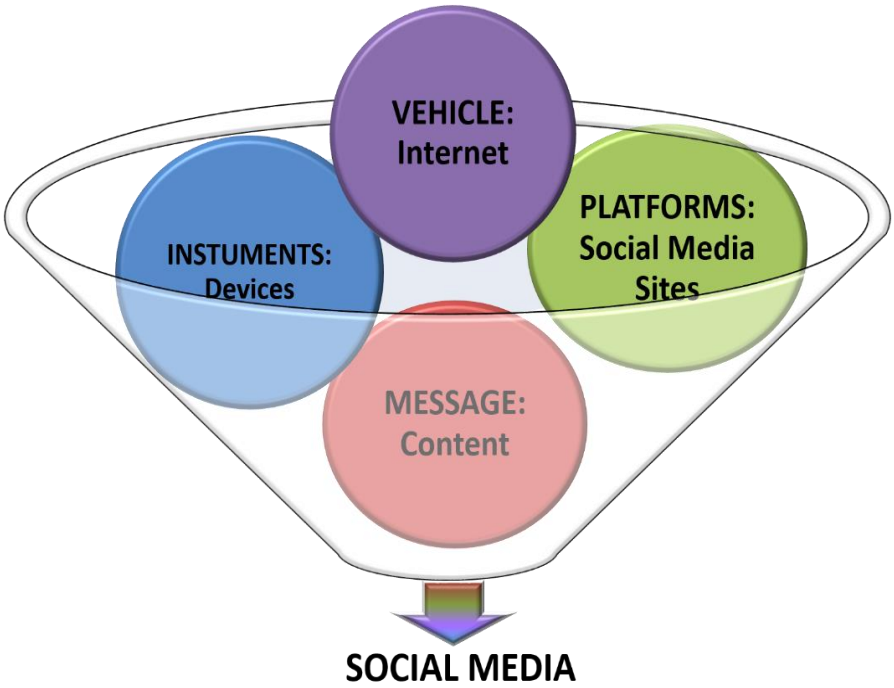
- Membership needs: The need to belong to a group and in this group comment on posts, add new content for comments by the group and use it to publicly agree or disagree with posts. This group also provides the opportunity for more visibility for content created online.
- Appreciation/esteem needs: Users feel appreciated by the number of invitations they receive to join a particular network.
- Self-fulfilment: Users make publicly known their personal qualities and according to these qualities, they can be contacted for advice and/or to join a group. A user can link up with a well-known or more visible user to increase their own number of contacts and profile.

In analysing literature pertaining to social media, it is clear that there is no single definition for this phenomenon. Furthermore, concepts such as social media and social networks are used interchangeably when referring to social media. It is therefore important to clarify these concepts to be clear what they mean, particularly in the context of this study.

Even though social media has been around for nearly two decades, there is still no commonly acceptable definition. The Merriam-Webster Online Dictionary (2004) describes it as "forms of electronic communication (such as websites for social networking and micro-blogging) through which users create online communities to share information, ideas, personal messages and other content (such as videos)". Boyd (2009:1), Schram (2018:2) and Cohn (2011:1) describe it in a similar way. Boyd (2009:1) describes social media as "the collection of software that enables individuals and communities to gather, communicate, share and in some cases collaborate and play" and Schram (2018:2) and Cohn (2011:1) define it as a platform that uses online technologies to enable interactive multi-media dialogue. On the other hand, Gupta (2013:18) labels it more broadly as "all devices (computing technologies such as the mobile phone) and platforms (virtual space where users come together such as Facebook®) that allow users globally to virtually create and share information with each other". While Gupta (2013:18) uses a more elaborate definition, other authors use simple description such as "the media we use to be social" (Safko, 2012:3), "array of new Web 2.0 platforms" (Schein *et al*., 2010:5) and "interactive digital tools that content users may generate, manipulate or influence" (Fraustino *et al*., 2012:7). From this discussion and for the purposes of this study, social media can be defined as the set of web-based broadcast technologies that enable people to communicate and to develop from consumers of content to creators of content.

With this understanding of social media as basis, the concept of social networking should be clarified. As highlighted earlier, social media and social networks are used interchangeably, but these two concepts do not have the same meaning. Social networks are viewed as a form of social media (Mayfield, 2008:6). Social media includes social networks, blogs, wikis, podcasts, fora, content communities and micro-blogging (Schram, 2018:2; Mayfield, 2008:6). According to the Merriam-Webster Dictionary (2018), a social network is "1) a network of individuals (such a friends, acquaintances, and co-workers) connected by interpersonal relationships; and, 2) an online service or site through which people create and maintain interpersonal relationships". Schram (2018:2) and Cohn (2011:1) describe social networks as a community that forms around a common interest. For the purposes of this study, social networks are defined as networks of individuals linked online along the lines of specific and common interests.

When examining the definition of social media, it is clear that it can be divided into four components: the digital technology, the internet, which is the vehicle of social media; mobile phones, computers or other communication devices, which are the instruments of social media; the social media sites, which are the platforms for social media; and then the message or the content that is communicated. This explanation of the four components of social media is depicted in Figure 49 below.



Source: Own construct

Figure 49: Components of Social Media

With the definition of social media clarified, it is also important to discuss the characteristics that distinguish social media from other media. According to Safranek (2012:2), Omede (2015:275), Montagnese (2012:5–6), Boyd and Ellison (2008:211) and Schein *et al*. (2010:4) the characteristics of social media include the following:

- Interactivity: One of the most important characteristics of social media is its high level of interactivity (see Chapter 4, Section 4.5.3). Kiousis (2002:372) describes interactivity as "the degree to which a communication technology can create a mediated environment in which participants can communicate (one to one, one to many and many to many) and participate in reciprocal message exchange". In relation to this study, social media is the communication technology providing the platform for communication. This interactivity distinguishes social media from traditional media (newspapers, radio and TV), where communication is only one-way. It allows for people to raise their opinions and comment on issues they deem important. Media messages are no longer a one-way communication; it has evolved into a dialogue between users. It is exactly this feature that also allows for the harvesting of these interactions for intelligence purposes (this is explained in greater detail in the section on SOCMINT).
- Availability: The information is immediately available. This is referred to as the viral[48] nature of new media in general and social media in particular. Once the information is posted on the social media websites, it is immediately available to users on that site.
- Cheap: Social media is cheap, and users can get results without investing a lot of money in communication infrastructure.
- User-friendly: The users can manage their own profiles and have the option to make it public or not. The users do not need advanced computer skills to use these applications.
- No censorship: Social media has created a channel for users to spread news and "bypass" the censorship and control that governments usually place on the media. This implies that information distributed via social media is not verified and false information can spread in this manner.
- Actions against big role players: A small or medium-sized group can launch harmful operations against bigger and more powerful competitors (for example, terrorist organisations against the United States of America).

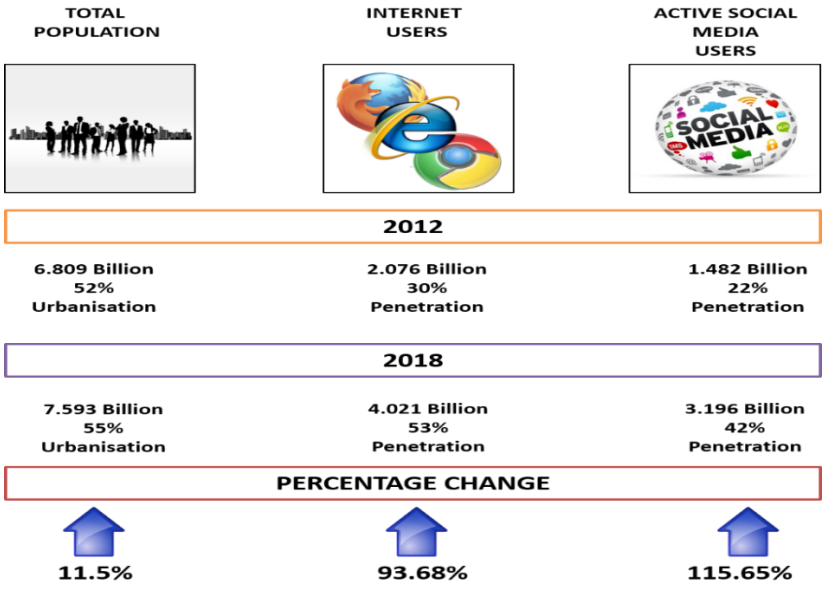
[48] Viral is deducted from the word virus, which refers to a small infection that can spread quickly. It refers to content that can spread quickly as it is electronically distributed from one person to another (Moreau, 2018:1).

The mass communication tool of social media is characterised by global transmission and an increased level of use mainly because of its handiness, flexibility and cheapness. As individuals, companies and governments constantly desire to interact with one another, online social networks are becoming a major growth point on the internet. This in turn has a positive impact on the development of the internet to deliver the network capabilities. Characteristics such as availability, cheapness and the enormous audience social media can reach make it a tool of choice for radicals.

With the history of the internet and the concept of social media defined, the next section describes the global digital landscape, which is a combination of these two elements.

7.4 Global digital landscape

Worldwide internet use has ballooned over the past six years from 2012 to 2018 (We are Social & Hootsuite, 2018:7). For the purposes of this study, there are two specific figures that are of great importance: the internet users and the active social media users. Both these figures increased substantially from 2012 to 2018 (Figure 50). The number of internet users increased by 93.68%, while the number of social media users increased by 115.65% (We are Social & Hootsuite, 2018:7). The growth over the past six years can be attributed to the improvement in technology across the globe, which enlarged accessibility and bandwidth (Kemp, 2018:1). This trend is expected to continue as technology development increases and reaches less developed regions.



Source: Adapted from We Are Social & Hootsuite, 2018

Figure 50: Global digital growth: 2012-2018

The development of the internet created the opportunity for new digital communication applications such as social media. As mentioned earlier, the first social network, SixDegrees.com, was launched in 1997 and included bulletin boards, e-mailing and online messaging between users with similar interests (Boyd & Ellison, 2007:214; Brunty *et al*., 2013:2). The use of social media started in more developed countries towards the end of the previous century. This was mainly as a result of the high technology development and the freedom of speech and communication in those countries. While the use of social media began in the developed world, it has spread to less developed regions across the globe. This is evident from Table 7 below where the penetration of 2018 is indicated. In 1997, when social media first started, penetration in less developed regions was 0%.

Table 7: Social media penetration as per region in 2018

REGION	SOCIAL MEDIA PENETRATION 2018
North America	70%
Africa	15%
South America	63%
Europe	53%
Asia-Pacific	42%
Middle East	52%

Source: Adapted from We Are Social & Hootsuite, 2018

While it is important to be aware of the increase in social media users, it is equally important to know which social network sites are the most popular and how this popularity is distributed across the various regions. This information is especially significant and useful to intelligence organisations, as this can give an indication of how the collection resources should be distributed. We Are Social and Hootsuite (2018:59) indicated in January 2018 that there were 2.167 billion Facebook® users, 1.5 billion YouTube™ users, 800 million Instagram™ users and 330 million Twitter® users.

Source: Adapted from Kallas, 2018

Figure 51: World map of social networks: 2018

With regard to the popularity of social media sites, Figure 51 depicts the situation in 2018. According to the map, Facebook® is dominant in the western countries and in Africa, the Middle East and the Pacific region. The social media in Russia is dominated by V Kontakte (supports the Cyrillic alphabet and is strongly directed at the Russian-speaking community). However, Facebook® is also growing in popularity. Twitter® is the dominant social media platform in Japan because it provides users with the anonymity they prefer while online (Kallas, 2018). As Facebook® is banned in China, Qzone is the most used platform. Currently Qzone has over 653 million users. Facebook® was banned in 2009 after the riots in Xinjiang province, because the activists used Facebook® to communicate and organise the riots (Kallas, 2018). However, the riots did not play the main role in the banning of Facebook®; it would have been banned anyway, as Facebook® did not adhere to government regulations in relation to content filtering (Kallas, 2018).

When analysing the internet and social media data for the past five years, it is clear that this phenomenon is snowballing and spreading across the globe. It is also expected that this trend will continue in the future as technology development in developing countries increase and internet access and bandwidth improves.

The discussion above has painted a picture of the internet and social media landscape globally. All indications are that the phenomenon of social media is spreading at a huge pace across the globe. It is therefore important to explain the threats and opportunities of this occurrence.

7.5 Social media application: threats and opportunities

Since the end of the Cold War, communication technologies have increased and connectivity (internet, mobile phones, computers and other electronic communication devices) have become a part of everyday life. These digital technologies empower people to connect with each other, to create value through online conversation and collaboration, to share different kinds of content (videos, photos, images, texts, sounds, etc.), to build/strengthen networks in one or more fields (professional, familiar, social, cultural, religious, political, etc.) and to develop and define their social identity (Scott & Jacka, 2011:5). The internet has changed the communication landscape to such an extent that a new contested space (cyber space) has been added to the security environment. The internet is a way of communicating with a person or with a range of people all at once and without taking boundaries into consideration. Furthermore, it is a powerful instrument to distribute information immediately to a huge number of users.

The substantial internet and social media growth rates, as discussed in the previous section (Section 7.3), lead to a growing amount of user-generated content reaching a greater number of users at a faster rate. As a result, social networking applications are becoming increasingly effective as an information facilitator and distributor. Over the past 20 years, social media such as Facebook®, Twitter®, YouTube™, Instagram™ and other social networking sites have ingrained their position in many users' daily activities, which saw these social media sites become a primary vehicle for political revolutions in countries such as Egypt (Eaton, 2013:19) and Tunisia (Howard *et al*., 2011:8).

This phenomenon has profound implications for security sectors all over the world. The application of social media can cause several negative effects for national security and unfavourable consequences for a state's strategic interests. These implications are negative in the form of threats, but also positive with regard to opportunities. The next section focuses on the threats posed by social media.

7.5.1 Social media: threats to national security

Except for the individual social and business uses of social media sites, there are bigger and more dangerous criminal uses of these sites that are of interest to the intelligence community. The following threats to national security can be identified:

- Terrorism: It is recognised that many terrorist and extremist groups use the internet and tools relating to the internet (Facebook® and YouTube™) for psychological warfare, publicity, propaganda, data mining, fundraising, recruitment, mobilising, networking, sharing information (for example, making of bombs and suicide vests), planning and coordination (Kohlmann, 2006:116; Montagnese, 2012:16-18; Theohary & Rollins, 2011:2; Thompson, 2011:168; Weimann, 2004:5-11). The internet is a strong propaganda tool for terrorist organisations. Terrorist organisations distribute videos of successes over the internet, which is a quick way of reaching millions of people. Previously, these organisations used middlemen to distribute the material. However, this practice was dangerous, as the men ran the risk of being caught. The first terrorist organisation to use the internet as a method of information distribution was Al Qaeda (Iraq, 2004) with the beheading of the American businessman, Nicholas Berg (Kohlmann, 2006:117). Social media helps terrorist organisations to distribute their material to a wider audience, attracting more followers.
- Criminal activities: Criminal organisations use social media sites to conduct their illicit activities (Montagnese, 2012:16–18; Theohary & Rollins, 2011:4). Activities include child pornography, drug smuggling, human trafficking, money-laundering and industrial espionage. These activities are increasing mainly because of the low risk of being discovered. According to Theohary and Rollins (2011:2), “cybercrime has surpassed international drug trafficking as a terrorist financing enterprise”. Abdulhamid *et al*. (2011:14) are of the opinion that social networking sites are a big threat to information security as these sites are open and accessible by known contacts and strangers alike. Individuals lose a substantial amount of their privacy online (Aronson & Cowhey, 2015:27). This openness has resulted in the rise of cybercrime that has implications for national security. According to Brunty *et al.* (2013:2), some of the criminal uses of social media include:
    - Twenty-first century burglary: stealing of personal information through the use of the internet.

    - Social engineering: Using information on the social media websites to lure a person to access a particular website containing malware[49] or to open an e-mail with malware. The malware gives the hacker access to the user's computer.
    - Phishing: Gathering information by means of a website that looks legitimate to obtain information such as account details, passwords and personal details.
    - Malware: Software installed unknowingly to gain access to personal information.
    - Identity theft: Criminal organisations can use personal details of users on social media to steal their identity.
- Protest movements and revolution: Revolutionary groups use social media such as Facebook®, YouTube™ and Twitter® as an organising tool to mobilise and manage activities with regard to issues of common interest (for example, the Tunisia and Egypt mass actions) (Montagnese, 2012:19). Social media is a powerful tool to organise people for a specific cause. The fact that social media is not restricted to geographical borders makes it even more powerful. Social media is a new mode of communicating information (positive or negative) quickly and to a great number of people. According to Montagnese (2012:19), social media is gaining recognition as an important element in the successful conclusion of protests and revolutionary activities. Papic and Noonan (2011:1–7) studied the phenomenon of social media as a tool for protests and they concluded the following:
    - There has been a noticeable increase in the use of social media by revolutionary groups, especially to spur disobedience and to manage protests.
    - The social media sites together with mobile phones guarantee the immediate spread of information, moving masses into action.
    - The use of social media lowers the cost of participation, training and organising, which makes it an important tool for protest movements that do not always have funds to mobilise masses.
- Careless use by civil servants: Social media users within government departments are also targets by virtue of their access to sensitive government information (Montagnese, 2012:20). This information can be accessed through criminal activities mentioned earlier, such as malware, social engineering and phishing. It is imperative that government departments (especially strategic departments such as SSA, Department of International Relations and Home Affairs) have a policy in place to ensure that sensitive information is not compromised.

[49] Malware is an abbreviation for malicious software, designed to attack computers (viruses and worms) (Clarke, 2012:81).

- The spreading of “fake news”: For the purpose of this study, fake news is the deliberate spreading of misinformation via the media (Cambridge Dictionary, 2018). The spread of fake news is made easier by social media sites. It was an important point of discussion during the 2016 election campaign in the United States of America, when Donald Trump accused journalists of spreading fake news. South Africa is also dealing with the issue of fake news. The Minister of the SSA indicated that there is an urgent need to regulate social media due to the rise in fake news, among other things (Dolley, 2017:1). The 2017 elections in Kenya also witnessed the occurrence of fake news. A message was distributed that the incumbent, President Uhuru Kenyatta, was ahead in the polls, when in actual fact the two candidates were neck-and-neck (Sevenzo, 2017:1, Cornish, 2017:1). The existence of fake news makes it important to cross-reference and verify information from social media, especially in the intelligence environment. In an effort to counter fake news, the Malaysian government passed an Anti-Fake News Bill earlier in 2018 (Gross, 2018; Sipalan, 2018).
- Propaganda: An issue that is closely linked to fake news is propaganda. Fake news can be used as a tool for propaganda. The use of a narrative (true or false) to change and influence people’s opinions and views has been used widely by governments and non-government organisations in their propaganda campaigns (Rickli & Kaspersen, 2016). Social media with its quick transmission and wide reach is a perfect tool in modern propaganda campaigns and has made influencing and deception of opponents easier.

This section highlighted the threats of social media to national security. However, social media is not only a threat, but can also be applied to support national security and the strategic interest of the country. The next segment highlights these opportunities.

7.5.2 Social media: opportunities for national security

Social media threats to national security are more noticeable, but it is also important to highlight the opportunities for national security. According to Montagnese (2012:21–28), these opportunities include the following:

- Crowd-source information: This refers to better flow of information from citizens to government agencies, with specific reference to emergencies. The 2010 Haiti earthquake is a good example. The earthquake severely damaged traditional communication methods and social media was used to organise humanitarian efforts across the country (Dugdale *et al*., 2012:1).

- Research, understanding and insight into groups: Researching social media could lead to a better understanding of various issues relating to social interaction and behaviour, especially radicalisation. Social media can help us understand political and radical groups suspected of illegal activities. The monitoring of social media will enable the security environment to recognise signs of hostile or potentially dangerous activities and provide early warning to government.
- Near real-time situation awareness: Social media can assist in creating a picture of the unfolding of events. During the Haiti earthquake, social media assisted the humanitarian efforts to get a picture of where assistance was needed (Dugdale *et al*., 2012:1).
- Influence, propaganda and deception: In the previous section it was mentioned that propaganda through social media has a negative impact on national security. However, social media can also be used by governments to influence political choices, decisions and behaviours of people by manipulating information, in other words propaganda (Bradshaw & Howard, 2017:3).
- Use in political campaigning: President Obama was the first presidential candidate to use social media in his campaign in 2008 and again during the 2012 campaign (Bogost, 2017).
- Institutional communication tool: Can be used in government between different departments to share information and interact with the public.

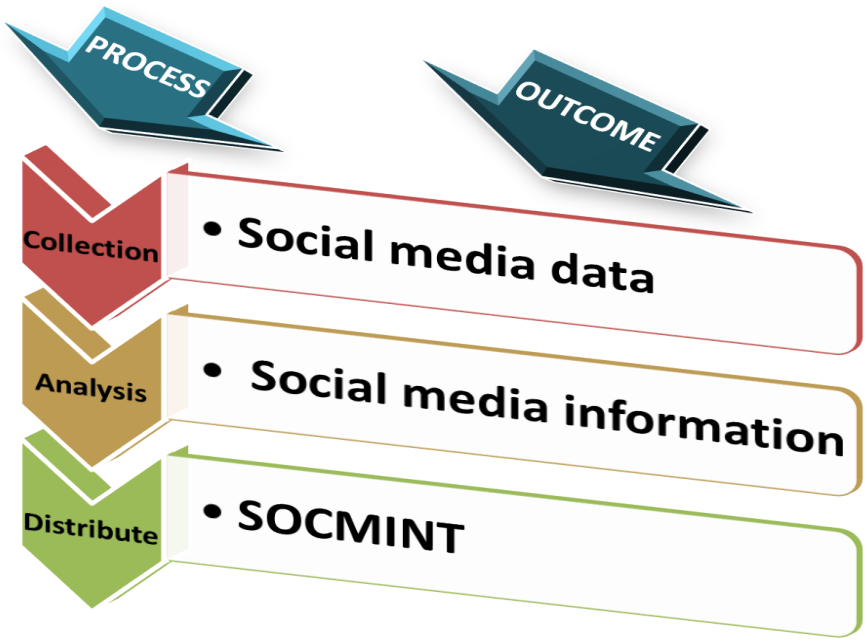
The above discussions clearly confirm that social media has national security implications. The borderless environment created by the internet and digital communication enables terrorist organisations or organised crime syndicates to communicate with current and potential members around the globe without taking any border requirements into consideration. Even though this phenomenon has negative implications, it can also play an important role in helping intelligence services to obtain important information. The information generated through social media platforms provide intelligence organisations with valuable information about organisations and people involved in illegal activities (SOCMINT).

From this section it is clear that social media has unquestionable national security implications and it is therefore of great importance to investigate how intelligence obtained from social media could be applied in the intelligence environment. The next section considers SOCMINT as an important source of information.

7.6 SOCMINT: applications and challenges

The term SOCMINT was first coined by Omand, Bartlett and Miller in a 2012 Demos report, #Intelligence, where the authors argue that this is a new and powerful tool for intelligence collection (Omand *et al*., 2012b:9). Marcellino *et al*. (2017:iii) concur and underline the fact that social media has the potential to support military operations because it provides a "window in the perspectives, thoughts and communications of citizens". Fitsanakis and Bolden (2012:28) refer to social media as "the new cutting edge in open-source tactical intelligence collection".

The term SOCMINT is increasingly being used as a new type of intelligence together with the existing family of sources: OSINT, HUMINT and SIGINT (see Chapter 5 Section 5.3.1 of this study for discussion on these sources) (Liaropoulos, 2012:6; Lombardi *et al*., 2016:1; Omand *et al*., 2012b:801). In a report by Marcellino *et al*. (2017:iii) it is stressed that the role of social media in military information operations is increasing because the users (allies and adversaries) are sharing information and influencing other users through social media platforms. SOCMINT is intelligence obtained from the analysis of information collected from social media interaction on social media platforms (the process is explained in Figure 52). The raw social media data are collected, analysed and the product, SOCMINT, is distributed to the client.



Source: Adapted from Farzindar & Inkpen, 2015:6

Figure 52: Social media analysis

There is currently a debate on whether SOCMINT should be viewed as a sub-section of OSINT or as a separate category[50]. An issue that complicates this debate is that SOCMINT can be open (publicly available) or secret (not publicly available) and does not easily fit into open or secret category of intelligence (Bartlett & Miller, 2013:14). Before the arrival of the internet, OSINT was defined as "information, lawfully obtained from overtly available sources such as newspapers, journals, books, conferences and government reports" (DCAF, 2006:2; Jensen *et al*., 2013:8; Liaropoulos, 2013:10; Shulsky & Schmitt, 2002:11). However, with the introduction of the computer and the internet the definition of OSINT changed to include "computer-based information" (Lowenthal, 2006:101). What then is the distinction between SOCMINT and OSINT? According to Bartlett and Miller (2013:14), the difference is found in the content and complex techniques needed to weigh the relevance of the information. The author of this study subscribes to the notion that SOCMINT differs from OSINT and should therefore be viewed as a source type on its own.

Although there is no consensus on the issue of SOCMINT and OSINT, there is strong agreement that the collection of SOCMINT is of great importance to the intelligence community (Liaropoulos, 2013:10; Lombardi *et al*., 2016:1; Omand *et al*., 2012a:801). This is especially pertinent in the new digital age where the intelligence community has to compete with the media, think tanks, private sector analysis firms and social networks. The intelligence services constantly have to examine how to remain relevant to the policy process and in the digital world of today. This also relates to SOCMINT. In this era of global news agencies, intelligence reporting lags behind the media by hours to days. Media reporting in turn lags behind social media reporting by hours (Steinitz & Zarin, 2012:3). This implies that intelligence organisations will be lagging further and further behind if they do not embrace SOCMINT. The Arab Spring is a case in point where the intelligence community could not provide relevant intelligence nor predict the outcome of this event because they did not understand social media and its application during social protests (Liaropoulos, 2013:11; Rovner, 2013:261).

The internet and social media platforms have created a community of users that are comfortable with sharing personal information online. The information on YouTube™, Twitter®, Facebook® and blogs provide useful tactical information for the intelligence organisations regarding users. This information includes habits, interests, causes they

[50] Another interesting angle is that of Lombardi *et al*. (2016:4) that SOCMINT and HUMINT should be combined to form DIGITAL HUMINT. This is an interesting view that should be pursued. However, this does not fall within the scope of this study.

support, social trends, associations, networks, other members of the network and public mood (Marcellino *et al*., 2017:7; Morozov, 2011:166; Steinitz & Zarin, 2012:3;). With this information social media creates the opportunity for companies to develop programmes to mine data to obtain information. Furthermore, social media platforms offer application programming interfaces (APIs) that assist with the harvesting or mining of data for the purposes of analysis (Bartlett & Miller, 2013:16; Williams *et al*., 2013:469). The Collaborative Online Social Media Observatory[51] is the first platform to integrate social media analytics with secondary data from all other sources (Williams *et al*., 2013:479).

Although law enforcement agencies and intelligence organisations[52] have been slow to react to social media and its potential intelligence value, the Arab Spring and other events (to be discussed later in this chapter) have forced action in this regard. Law enforcement is increasingly using software to capture relevant information from social media sites (termed "dataveillance") in the monitoring of criminal groups and gangs (Brunty *et al*., 2013:89–90; Moe & Schweidel, 2014:7). According to SAS (2012:5–7) and Marcellino *et al*. (2017:7–8), the information obtained from social media is obtained by means of software that assists with:

- analysing key elements and significant text;
- analysing sentiment – although programmes have been developed to do mining, the gauging of sentiment is still not sufficient and analysts remain the best way to examine social media to determine sentiment (Moe & Schweidel, 2014:10);
- identifying relationships and patterns within relationships;
- language translation; and
- categorising messages into subjects or categories.

Against this background it is important to note that SOCMINT consists of different types of information. According Bartlett and Miller (2013:14–15), the following types of SOCMINT can be identified:

- Natural language processing: This is a branch of artificial intelligence that analyses the interaction between human language and computers. It entails using computer programmes to understand, analyse and develop meaning from human language and

[51] COSMOS is an initiative with input from various disciplines (social, health, computer, statistics and mathematics) that analyses social media data for policy purposes. COSMOS is based in the UK and consists of collaboration between Cardiff, Warwick and St Andrews Universities.

[52] The Federal Bureau of Investigation employs the private sector to develop new software to assist with the mining and analysis of social media data (Ungerer, 2012:1).

specifically in SOCMINT as it transpires in social media. The tasks include summary, translation, relationship extraction, sentiment analysis and speech recognition.

- Event detection: Through the analysis of SOCMINT, planned events can be identified.
- Data mining and predictive analytics: Analysing social media data to find connections and interactions.
- Social network analysis (SNA): Through the use of applications based on mathematical techniques, characteristics of the network structure, such as connections, the structure of the network and type of network are found.
- Manual analysis: Netnography is the "application of ethnographic and qualitative sociologies to the study of social media" (Bartlett & Miller, 2013:44).
- Solicited/'crowd sourced' insight: Directly requesting information from users. The social media users are requested to provide their data (pictures and videos) to compile a picture of an event. The users are viewed as sources of information.

The above-mentioned SOCMINT could assist the decision-making process with regard to policy changes or implementation. However, it is important that this information be timely and correct.

The collection of SOCMINT is done through various methods and techniques. Bartlett and Miller (2013:16–49) highlight the following techniques and methods to obtain SOCMINT:

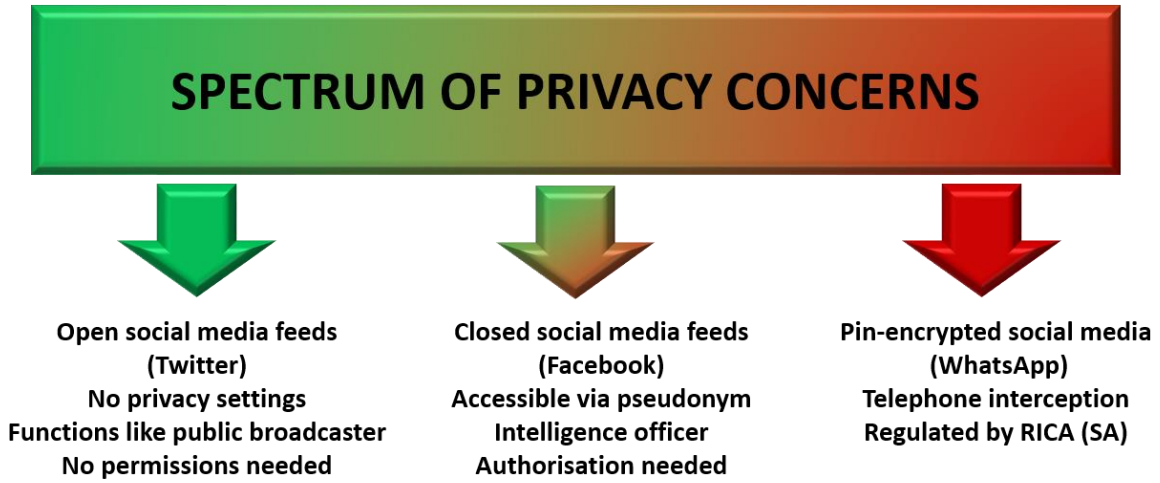
- Social media data collection and retrieval: As a result of the amount of social media data available, it is difficult to manually collect the data. It is important that this data be collected automatically through the API of the social media platform. Information that can be obtained from this application includes geo-location, time zone and creation data of the user.
- Web scrapers and crawlers: These are automated programs that are applied to find and catalogue information stored on websites. Crawlers follow hypertext links from one site to the next and records the links to the sites.
- Information retrieval: In this case information is obtained by means of retrieval software that works through rules-based algorithms. It is important that the retrieval ware can search across the spectrum of multimedia, which includes text, pictures and videos.
- Machine learning/natural language processing: This is a sub-field of artificial intelligence and combines approaches in the fields of computer science, applied mathematics and linguistics to detect the meaning of natural language as found on social media.

    - Attitude data/sentiment analysis: This information can assist in determining the sentiment or mood of the people and will make it easier to predict social unrest and illegal actions.
    - Latent insight: Analysing the data that is not in the text such as the age, gender and location.
- Event detection and situational awareness:
    - Situational awareness via Twitter®: Events are reported on Twitter® as they occur. Users create first-hand information about an event; they can request information, add additional info and resend info. The multimedia capacity (photos, maps and sound) of social sites adds useful information and helps characterise events. Furthermore, this data provides more legitimacy to the information. An important prerequisite of event detection technology is to verify the credibility of information with regard to a specific event.
- Predictive analytics: The big data landscape is making predictions possible. The social media phenomenon is also exacerbating the revolution of big data. Social interactions are increasingly being captured online through social media platforms. Bartlett and Miller (2013:31) call it the “datafication” of social life. Areas where predictive analysis can be used are in politics and in health (public health monitoring, tracking health trends) and crime detection.
- Network analysis (see Chapter 4, Section 4.5.3):
    - SNA is rooted in sociology and the mathematical disciplines. The aim is to distinguish the nature, intensity and frequency of social ties, working on the supposition that social ties influence people, their beliefs, behaviour and experience. Through the mathematical measuring and mapping of these ties the analysis attempts to explain and predict behaviour of individuals within the network. The linkages focus on content, structure or usage and allow the analyst to build a dataset of activities across social media sites.
    - One of the important applications of SNA is to determine the strength of the relationships based on social media activities. This analysis can determine the level of influence a person has in a group.

      Another important area of interest with regard to SNA is the focus on the content of the information shared. This can highlight changes in a group’s beliefs and views. There are various programmes to measure this phenomenon.
- Netnography: This is the study of behaviours within an online community that could provide information with regard to attitude formation and behaviour.

- Crowd-sourced information: Social media is increasingly being used by users to directly ask for assistance (missing person). This is also a useful way of collecting data for surveys.

The discussions above elucidated the importance of SOCMINT and how it can be collected and applied. However, we should be cognisant of the fact that SOCMINT does have challenges that have to be taken into account. One of the first and perhaps the most important challenges of SOCMINT is related to legal aspects of intelligence collection (Omand *et al*., 2014:36; Marcellino *et al*., 2017:iii). As mentioned earlier, SOCMINT consists of open social media intelligence and secret social media intelligence. This has implications for the level of access to the information on the side of intelligence organisations and law enforcement agencies. Omand (2013) refers to three categories of access. The first is open social media feeds that have no privacy settings. The information is in the public domain and accessible to anybody. The second is semi-private information. Such information can be accessed by becoming a member of the closed group (deception). The third is secret information that implies interception and where access can only be granted by law (Figure 53).



Source: Adapted from Omand, 2013

Figure 53: SOCMINT privacy spectrum

Although various countries have legislation with regard to the access and interception of information, most of these laws were enacted before the existence of social media. In order to have access to the full spectrum of SOCMINT, laws and regulations should be amended to include social media websites (Brunty *et al*., 2013:90; Omand *et al*., 2014:36). Access to the internet has democratised information, making it less dependent on political

bureaucracy. Until the early 1980s most television stations in the world were government controlled and even the written media to some or other extent had to report to their political sponsors. This situation made it easy to regulate and control news and other items that were transmitted to the public. However, the technology revolution changed this situation and made regulation of information very difficult. The ability to instantly disseminate information in a viral fashion has created a very real dilemma for institutions and countries that require a degree of discretion to survive. The problem stems from the fact that it is not possible to police and control the entire internet nation.

It is difficult to regulate the internet in general and social media in particular. This is mainly because of a lack of agreement and cooperation among states on issues such as the governing body of a treaty (Wu, 2015:281). Some countries, such as Nigeria, have legislation to control social media, but these efforts are criticised for infringement on human rights (Omede, 2015:277). Other African countries, such as Cameroon, Chad, DRC, Gambia and Gabon, have blocked access to social media during elections (Cross, 2017:1). The issue of regulation has also been raised in South Africa. The recent unrests (student and service delivery protests) and the use of social media to mobilise the population as well as the spread of fake news has prompted the Minister of the SSA to call for the investigation into the regulation of social media (Herman, 2017:1). This was met with an immediate reaction by the social media community in South Africa with the *#HandsOffSocialMedia* campaign where various members within the social media community raised their dissatisfaction with the prospect of regulation in the social media arena (Van der Merwe, 2017:1).

The second important challenge is credibility (Omand *et al*., 2014:33). SOCMINT is a new type of intelligence and as of yet there are no criteria to test and evaluate its credibility. Criteria such as verification and how the information was gathered or obtained are of great importance to provide credibility to information before it can be used in the analysis process. The next important challenge is representivity (Omand *et al*., 2014:33). Social media analysis with the use of mining software provides large amounts of aggregated data. However, information received from the social media samples cannot be extrapolated to the bigger population because social media users are not representative of the whole population (Marchetti-Bowick & Chambers, 2012:611). Another challenge with regard to SOCMINT is accuracy (Omand *et al*., 2014:34). Social media and the software developed to measure activities on these platforms are new. The accuracy of these applications can only be tested and corrected over time. The measurements are done by software and computers and the human aspect is not taken into account. A fifth challenge is authenticity (Omand *et al*.,

2014:34). The anonymity of the internet in general and social media in particular creates an ideal environment for deception. It is extremely hard to detect deception online and to authenticate the information. The sixth challenge is reality (Omand *et al*., 2014:34). Information mined from social media sites does not include context, it only provides the outcomes. In order to be useful, it is of great importance to be aware of the context of the situations before conclusions can be made. For example, in January 2012 two British tourists were barred from entering the USA after joking they will "destroy America". Context would have shown that they were planning on having a good time. The final challenge is substantiation (Omand *et al*., 2014:34). Currently there are no strategies to test the validity or confirm the information on social media.

The global security environment is in flux. Since the beginning of time the global security environment has been changing as new security issues came to the fore as a result of new inventions and changed political situations. These changes to the security environment have exponentially increased over the past two centuries mainly as a result of the increase in the pace of technology development. New security threats have surfaced after the end of the Cold War largely because of ICT development. With the changing security environment, it is of utmost importance that intelligence organisations keep up with changes to safeguard national security. One of the most important changes over the past few decades has been the digital revolution. The digital revolution has democratised information in that not only do more people have access to information, they can also create new information. The increased use of social media by citizens to share information and organise activities against the state can be perceived as potentially dangerous to the state. SOCMINT is an important new source of information that can be applied together with the traditional sources, such as HUMINT, OSINT and SIGINT. SOCMINT provides the intelligence community with intelligence regarding social behaviour on cyber platforms. Intelligence has always been there to provide information in relation to national security. Social media is one more way of providing this information. However, this new source of information is still in its infancy. For it to be viewed as a credible and useful source there is a need to investigate and understand challenges such as reliability, authenticity, accuracy, application and regulatory implications. It is expected that intelligence organisations will increase social media monitoring to obtain information about terrorist networks and planning.

With this discussion of social media as background, the section below evaluates the value of SOCMINT during various events around the globe.

7.7 Global events and SOCMINT

There has been fervent discussion on the effectiveness and the impact of social media during the Arab Spring and other events (Liaropoulos, 2013:8-10; Shirky, 2011:1; Safranek, 2012:3; Thompson, 2011:177). Below are some of the important events that illustrate the use and impact of social media within the intelligence context.

- The Philippines 2001: Loyalists to President Joseph Estrada voted to set aside key evidence during his impeachment trial. Once this became known, activists mobilised a protest via text messages. Over a million people arrived for the protest actions in Manila. Legislators reversed the decision and the evidence was submitted (Liaropoulos, 2013:8; Safranek, 2012:3; Shirky, 2011:1). Following these events, President Estrada resigned on 20 January 2001. For the first time, social media helped to force out a national leader (Shirky, 2011:1).
- Mumbai attacks 2008: During the Mumbai terrorist attacks the offenders used cell phones to receive and send information in real time and watched the events unfold on the internet. During this time citizens were broadcasting the movements of the police over Twitter®, which negatively affected the police efforts to apprehend the assailants (Thompson, 2011:177). Social media was used both by the attackers and the citizens. The citizens used social media to see what was happening and in the process broadcast details of their locations. This information in turn was used by the criminals to find the hiding places of citizens to attack them (Thompson, 2011:177).
- Moldova 2009: Civil unrest broke out after the Party of Communists (PCRM) won the majority of the seats in the parliamentary elections of April 2009 (Liaropoulos, 2013:8–10; Safranek, 2012:3; Mungiu-Pippidi & Munteanu, 2009:136). Protests were sparked by the opposition accusing the PCRM of fraud (Mongiu-Pippidi & Munteanu, 2009:136). While the PCRM won 61% of the votes, they could not appoint the president (Mungiu-Pippidi & Munteanu, 2009:138). The unrest, together with the opposition's inability to select a president, resulted in a second round of elections in June 2009 (Dix, 2011:93; Mungiu-Pippidi & Munteanu, 2009:139;), which was won by a coalition of opposition parties (Dix, 2011:93).
- Iran 2009: The Green Revolution, as it was known, was the first major world event that used social media to gain international attention and action. However, it was not the most significant organising factor in the country (Liaropoulos, 2013:8). After the re-election of President Mahmoud Ahmadinejad, young Iranians claimed that the elections had been rigged and started a social uprising. During this uprising the Iranians used

social media, mainly Twitter®, to channel information about the protests. Iran engages in severe digital surveillance and online censorship and during the uprising the social network sites were blocked and those promoting the protests were identified by the intelligence organisations (Aday *et al*., 2010:13). As Facebook® and YouTube™ were blocked, the Iranians used Twitter® to send text messages with mobile phones. While the message about protests was communicated by word of mouth inside Iran, Twitter® was mainly used to make the international community aware of the situation in the country (Safranek, 2012:4; Liaropoulos, 2013:8).

- Tunisia December 2010: The revolution in Tunisia was also called the Jasmine revolution (Safranek, 2012:5). While Twitter® did not play a crucial role in the Iran uprising, the situation in Tunisia was different. Social media was responsible for the global attention to Mohamed Bouazizi's self-sacrifice (a 26-year-old fruit and vegetable seller who set himself alight) (Liaropoulos, 2013:9, Safranek, 2012:5). Images and videos of Mohamed's act and the protests were uploaded to social media sites and spread among the Tunisians with internet access and around the globe (Howard *et al*., 2011:8; Liaropoulos, 2013:9). The footage reached the Al Jazeera news channel, which broadcast it around the globe and amplified the plight of the Tunisian people. Most Tunisians did not have access to internet and could not participate by using social media. This, together with the efforts of the regime to curb the uprising and disrupt the flow of information by hacking of e-mails and Facebook® accounts, forced the citizens within Tunisia to turn to the use of television, a traditional media format. The social unrest lasted less than a month and resulted in the dictator, Ben Ali, leaving the country (Liaropoulos, 2013:9; Safranek, 2012:2). This event was a close collaboration between old and new media. Social media played a critical role at the beginning of the uprising and the initial spread of footage that eventually reached traditional media sources. This event and the use of social media changed journalism. During this time citizens were turned into journalists, broadcasting events through social media to the international users.
- Egypt: The Tunisia uprising was followed by the civil unrest in Egypt. The Egyptians started to protest against the oppressive and corrupt regime of President Mubarak and social media was used to communicate messages, online maps and encryption techniques (Liaropoulos, 2013:9). Facebook® pages such as "Information Age: Egypt's Revolution" were created to organise the population (Safranek, 2012:5). The Egyptian regime increased online censorship by monitoring e-mail accounts, social media networks and arresting dissidents responsible for coordinating protests. In an attempt to curb the protests, the regime decided to cut off the internet for a few days (Liaropoulos, 2013:9; Eaton, 2013:11). In spite of these actions, the message still reached the

population of Egypt and international support increased. The Egyptian people had to rely on alternative ways of communication. Satellite phones were imported and TV channels used alternative satellites for transmission to the people of Egypt (Liaropoulos, 2013:9). During this time Google® and Twitter® released a new social media tool *Speak2Tweet*, which was used to call a number, leave a message, where after this message would be tweeted on the Twitter® website (Liaropoulos, 2013:10; Safranek, 2012:5; Liaropoulos, 2013:9). As was the case in Tunisia, the combination of traditional and new media played a crucial role in bringing the revolution to the international community.

- London 2011: On 4 August 2011 the police fatally shot Mark Duggan, which sparked public protest across England (SAS, 2012:2; HMICFRS, 2011:5). During this time social media was utilised by the organisers of the protests to communicate plans and to mobilise members of the communities. The police were not equipped to tap into the social media data to analyse the information and was always lagging behind the plans of the protesters, which impacted negatively on their efforts to curb the protests (HMICFRS, 2011:6; SAS, 2012:2).
- Libya, Syria and Yemen: In these countries the internet penetration rate is low with a subsequent low number of social media users. This, together with the totalitarian regimes that foiled reform efforts could be why protests for political and social change were not successful (Safranek, 2012:5; Thompson, 2011:177).

In analysing these events, the following SOCMINT opportunities can be identified:

- In all these cases social media analysis (sentiment analysis) could have assisted the intelligence community in determining the mood and the level of discontent among the population. This analysis could have indicated that the citizens were becoming impatient with the political situation.
- In the terrorist attack in Mumbai the intelligence organisations could have used the information that was broadcast by the citizens to create a picture and track down the perpetrators.
- Intelligence organisations could have identified the main role players or organisers in the uprisings, their locations, and social links.
- Through analysing social media sites, intelligence organisations could have identified planned events and have mitigated the outcome of the event or have stopped the events from happening.

Events in a number of countries such as Iran, Tunisia and Egypt have clearly indicated that social media can play a crucial role in organising and mobilising political protests. As mentioned earlier, the effectiveness of social media and the role it played is widely under discussion. Social media provides a voice to mobilise the masses, gives communication capability, and raises awareness locally and internationally by reporting situations in real time as it happens (Eaton, 2013:11; Howard *et al*., Liaropoulos, 2013:7; 2011:5; Thompson, 2011:178). While some authors acknowledge that social media did not cause the revolution, they do suggest that it did augment and facilitate the democratisation efforts of protesters (Eaton, 2013:11; Howard *et al*., Liaropoulos, 2013:7; 2011:5; Thompson, 2011:178;). In contrast, Morozov (2011:ix–xii) strongly refutes the role of technology in sparking demonstrations and the eventual democratisation of communities. Instead, he views these new technologies as instruments in the hands of authoritarian government as they can be used against social movements to collect intelligence (Morozov, 2011:166–167). Although Morozov (2011:166–167) is correct in that these tools can be used to collect information on social movements, this study concurs with Howard *et al*. (2011:5), Thompson (2011:178), Eaton (2013:11) and Liaropoulos (2013:7) that social media, though not the cause of the uprisings, increased the effectiveness of the protests. It is therefore necessary to investigate and include SOCMINT as an important source of information within the intelligence environment.

It is important to highlight some critical conclusions. First, technology in general and social media in particular did not cause the events in Tunisia, Egypt and Iran, they just amplified the effectiveness. The underlying socio-economic and political situation in these countries caused these events and social media was merely the tool to ignite the situation. A second observation is that social media was crucial in the beginning stages of the uprisings to spread the message, provide information and mobilise part of the local population and raise international awareness. Both new and old media were used to spread the message and muster awareness. Third, social media has changed the face of journalism and every person with a smart phone and access to the internet can now be a journalist[53]. By applying the digital tools to bypass traditional media to distribute information, a wider audience is reached. This, however, has created the problem of fake news.

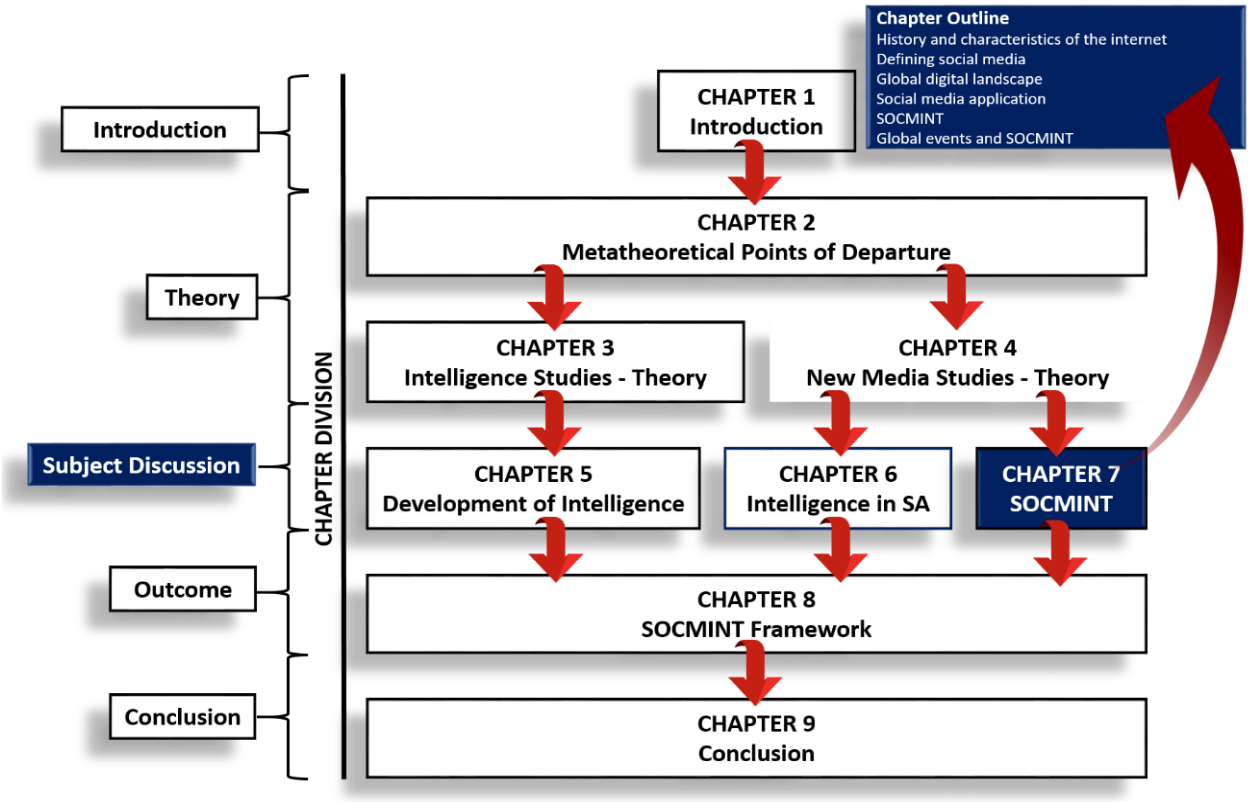
[53] The citizen journalist collects analyses and digitally distributes information and operates independently from news agencies (Rogers, 2018).

7.8 Conclusion

The main aim of this chapter was to explain SOCMINT and its applications in the intelligence environment. In order to reach this goal, the first step was to discuss the history of the internet. The second section of the chapter conceptualised the social media phenomenon and identified the threats and opportunities for national security. The digital revolution has brought with it a communication revolution called social media. This tool has fundamentally changed the way communication takes place across sectors (business, individuals and government). Social media is a communication tool characterised by global transmission and an increased level of use mainly because of its handiness, flexibility and extreme inexpensiveness. It connects like-minded people either to build friendships or to increase membership in support of a specific cause. The structure of the internet allows for malicious activity to flourish and perpetrators to remain anonymous (Kohlmann, 2006:116–124). The use of social media tools by individuals and organisations to radicalise individuals for political and social change has become increasingly popular as the internet penetrates further into the world. This phenomenon is growing day by day, increasing the threats to national security. It is not social media per se that poses a threat to national security, but the purpose for which it is used (Montagnese, 2012:7).

Finally, SOCMINT was conceptualised and its uses for the intelligence environment explained. Policy makers across the globe are operating in a real-time environment where the time that passes between decision-making and implementation is becoming crucial (Andrus, 2005:1). However, the changes in technologies are not equally matched by changes in the security and intelligence environment. Technology will continue to shape intelligence practices and competencies. A strategy is needed to manage the ever-increasing open-source information available by electronic means, such as social media. It is of great importance that the intelligence community transforms to dynamically reinvent, learn and adjust with the changing national security environment (Andrus, 2005:1). There is an urgent need for intelligence organisations to increase their capacity, both in social behaviour and technology, to analyse data from SOCMINT to provide intelligence to the policy making process.

Figure 54 below provides a summary of the chapter outline and its relation to other chapters in this study.



Source: Own construct

Figure 54: Chapter 7 Summary

Given this detailed background of social media and SOCMINT, the next chapter focuses on the social media landscape within the South African context and a framework for SOCMINT is developed.

CHAPTER 8: A FRAMEWORK FOR SOCMINT IN THE SOUTH AFRICAN CONTEXT

"When society develops and adopts new methods of communication and organisation – such as social media – public institutions, including the police and intelligence services, have a responsibility to react and adapt. The explosion of social media is the latest in a long line of disruptive technological innovations, and now requires a response from the authorities in turn."
(Omand et al., 2012a:804)

8.1 Introduction

The previous chapter provided a detailed discussion on the history of the internet and social media and how this new form of communication manifests in the global environment. The chapter also considered SOCMINT and concluded with a description of recent events where social media played a crucial role. With this as background, it is imperative to examine social media and SOCMINT within the South African context. This lays the groundwork for the strategic framework for the national security environment.

Goodman (2008:3) comments that "the world is less dangerous today than it was a decade ago". He bases his assessment on the fact that the end of the Cold War eliminated the USA's adversary and this implied a lack of a singular present danger (Goodman, 2008:3). However, since the end of the Cold War, the intelligence environment has changed dramatically. The security situation has become much more complex as a result of a range of new security issues such as terrorism, transnational organised crime, cyber warfare and cybercrime (Booth, 1991:314; Collins, 2013:289-379; Krahmann, 2005:4). The global landscape is constantly being changed by new technologies. This changing landscape and new security issues (some as a result of new technologies – cybercrime) complicate the security environment, resulting in a world that is undeniably less safe. The previous chapter focused on social media as one of the new communication technologies that has major implications for security around the globe. Omand *et al*. (2012a:804) refer to these new technologies as "disruptive" and highlight that there is a definite need for intelligence organisations to respond to the new communication developments.

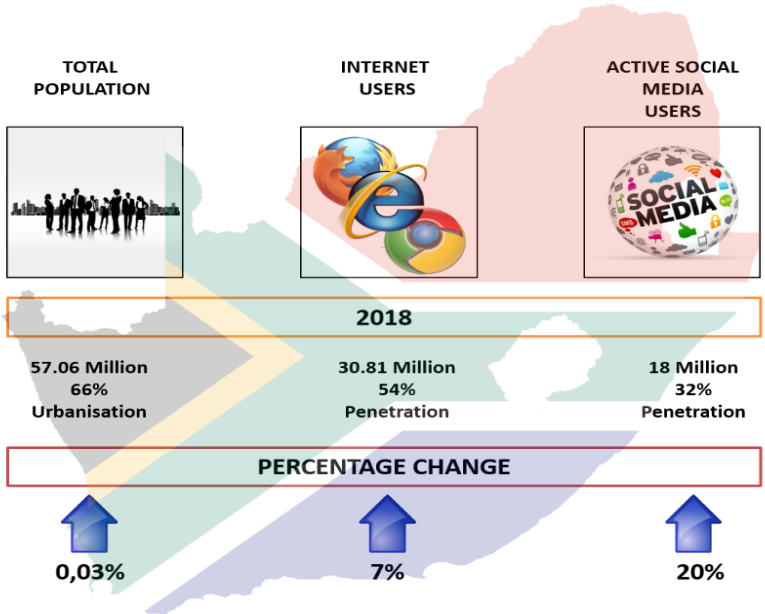
This chapter focuses on the South African social media environment and forms the background for the suggested strategic framework. First, the social media landscape in South Africa is described before discussing the manifestation of social media and the threats it poses. This is followed by the development of a strategic intelligence framework that

includes SOCMINT. As mentioned earlier, SOCMINT is currently not included in the South African intelligence framework. A framework is needed that includes SOCMINT to mandate and guide the collection process and its application within the intelligence environment. However, the challenge is to incorporate, apply and manage SOCMINT in the South African intelligence environment. SOCMINT's most important contribution will be to the collection environment as it is a new collection instrument. However, it is imperative that issues such as oversight and accountability be addressed before it can be viewed as a legitimate source of information. The chapter concludes with findings and recommendations in relation to SOCMINT within the South African context.

The discussion below builds on the information on the global social media landscape provided in the previous chapter and highlights the South African scene.

8.2 The social media landscape in South Africa

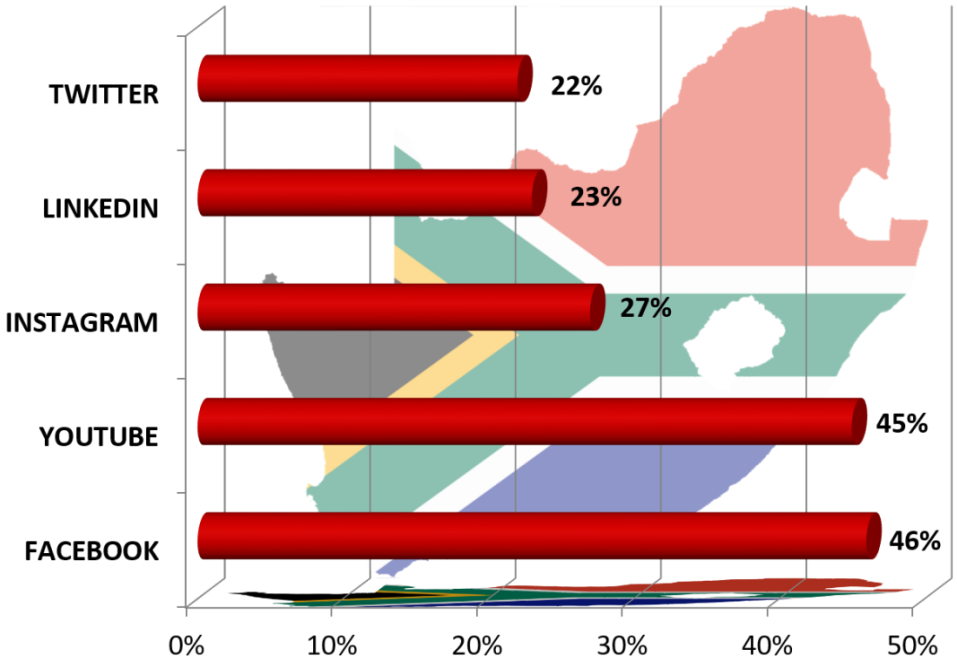
South Africa's digital picture is portrayed below in the various graphs. Of the 57.06 million people in South Africa, 30.81 million (54%) has access to the internet and 18 million (32%) are active social media users (Figure 55). In comparison to 2017, the number of internet users has increased by 7% in 2018, while the number of social media users has increased by 20% (We are social & Hootsuite, 2018:386). It is expected that these figures will increase even further as communication technology and bandwidth improve to reach more people in rural areas. These trends in South Africa are in line with the developments around the globe.



Source: Adapted from We Are Social & Hootsuite, 2018:133

Figure 55: South African digital growth: 2016-2017

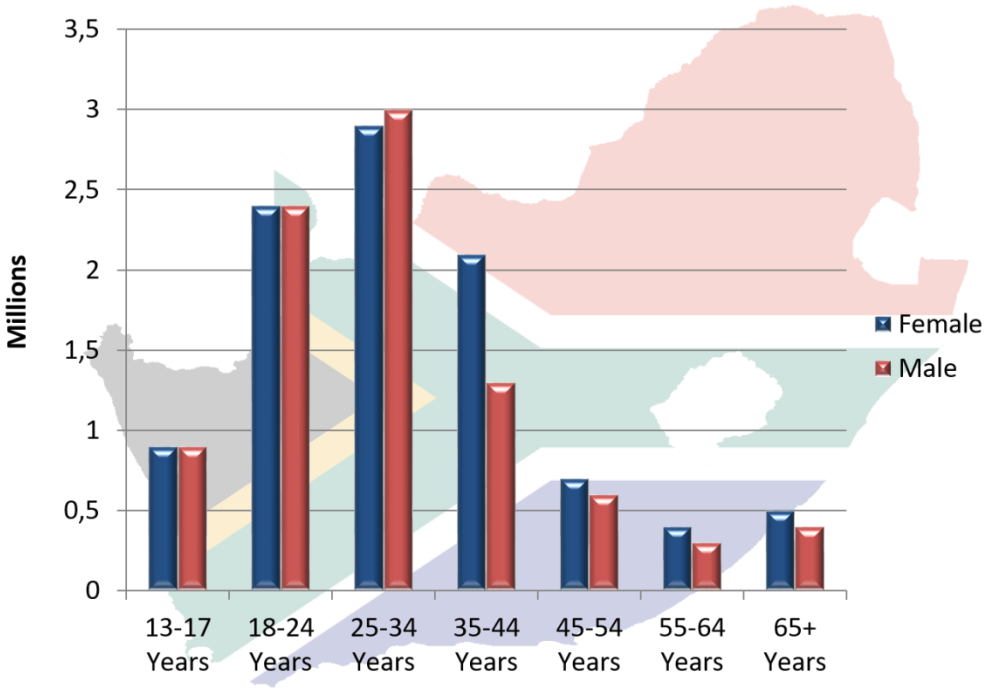
The most active social media network sites in South Africa are depicted in Figure 56. The graph indicates that Facebook®, YouTube™ and Instagram™ are the most important social media network sites (We Are Social & Hootsuite, 2018). Even though Twitter® is not among the top three sites, it is frequently used during social unrest as was evident during the #FeesMustFall campaign.



Source: Adapted from We Are Social & Hootsuite, 2018

Figure 56: Most active networking sites in South Africa

The profile of Facebook® users in South Africa is illustrated in Figure 57, which is another significant indicator. Facebook® is the most frequently used social media site in South Africa and it is therefore important to demonstrate the breakdown of the country's Facebook® users by age and gender. According to this graph, the youth (18–34) are the most dominant users of Facebook® and the distribution between male and female is almost equal (2.4 million female and 2.5 million male). As already indicated in the previous chapter, the use of social media is increasing globally and in South Africa. However, from an intelligence perspective in the case of South Africa, the high youth unemployment rate (51% – Trading Economics, 2018) together with the high Facebook® use among this age group is disconcerting because this group can easily be mobilised around issues as they are already part of the social media community.



Source: Adapted from We Are Social & Hootsuite, 2018

Figure 57: Profile of FB Users in South Africa

With the social media landscape explained, it is vital to also highlight how social media features within the South African context. The next section describes how social media has affected national security.

8.3 The manifestation of social media and its threats in the South African context

Social media is widely used across the world and in South Africa. However, it is imperative that the manifestation of social media use be contextualised in the South African environment. The framework used to measure a threat to national security is explained first so that we would be able to evaluate the threat implications of social media in the South African context.

The framework to measure implications to national security is found in the General Intelligence Laws Amendment Act (11 of 2013), which states that “national security includes the protection of the people of the republic and the territorial integrity of the Republic against-

(a) The threat of use of force or the use of force;

(b) The following acts:

(i) Hostile acts of foreign intervention directed at undermining the constitutional order of the Republic;

(ii) Terrorism or terrorist-related activities;

(iii) Espionage;

(iv) Exposure of a state security matter with the intention of undermining the constitutional order of the Republic;

(v) Exposure of economic, scientific or technological secrets vital to the Republic;

(vi) Sabotage;

(vii) Serious violence directed at overthrowing the constitutional order of the Republic;

(c) Acts directed at undermining the capacity of the Republic to respond to the use of, or the threat of the use of, force and carrying out of the Republic's responsibilities to any foreign country and international organisation in relation to any of the matters referred to in this definition, whether directed from, or committed within, the Republic or not, but does not include lawful political activity, advocacy, protest or dissent."

The above-mentioned definition must be read in conjunction with the Principles of National Security as set out in the Constitution of the Republic of South Africa (1996:103). According to the Constitution (1996:103), "national security reflects the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life". The most important part of this principle is "to live in peace" and "free from fear". According to the General Intelligence Laws Amendment Act (11 of 2013), South African intelligence agencies are mandated to protect the citizens and the territorial integrity of the country.

When analysing the use of social media in South Africa measured against the threats discussed in Chapter 7 (7.5.1) and the national security framework (discussed above), three specific threats are observed. The first is in relation to the protest movements and a revolutionary threat, as witnessed in the various Twitter actions. On this matter, the first such movement was the #RhodesMustfall in early 2015. A student from the University of Cape Town (UCT) started the #RhodesMustFall movement to take down the statue of Cecil John Rhodes (a perceived symbol of colonialism) on the campus of the University of Cape Town (Breakey, 2017; Etheridge, 2016; Hodes, 2015). This protest resulted in the removal of the statue in 2016 (Etheridge, 2016). Following this movement was the #FeesMustFall campaign towards the end of 2015 (Breakey, 2017; Maseko, 2016; Mulambo, 2017; Thomas, 2015).

The #FeesMustFall movement started at the University of the Witwatersrand (Wits) in October 2015 against the proposed increase (11%) in tuition fees (Breakey, 2017; Thomas, 2015). The movement quickly spread to other universities across South Africa (Thomas, 2015; Breakey, 2017). The result of the protests was the announcement by President Zuma that there would be no increase in fees for the 2016 academic year (Thomas, 2015). Other movements were the #ZumaMustFall and #SaveSA in response to the corruption scandal surrounding President Zuma (Sangham, 2017). While these movements did not produce the anticipated outcome (the President's resignation), it did highlight the negative perception towards the President. Although the General Intelligence Laws Amendment Act (11 of 2013) does not view lawful protests as a threat to national security, the actions (violence, intimidation and damage to property) during these protests can be regarded as "overthrowing the constitutional order of the Republic" and pose a threat to national security.

The second threat that manifested in the South African social media landscape is the use of social media as a propaganda tool. A perfect example of such a propaganda campaign is that driven by Bell Pottinger. This British public relations company was hired by Oakbay Investments and the Gupta family to counter negative publicity after the release of the Public Protector's report on state capture[54] (November 2016) (Testa, 2018; Umraw, 2017:1). The company used social media campaigns such as the "white monopoly capital" idea to draw attention away from the Gupta and President Zuma scandals (Testa, 2018; Umraw, 2017:1; Writer, 2017). When the relationship between Bell Pottinger and the Gupta family surfaced with the leaked Gupta e-mails, South Africans were furious and as a result of a social media backlash, Bell Pottinger was forced to publicly apologise for their actions (Testa, 2018). The Democratic Alliance submitted a complaint regarding this issue to the UK-based Public Relations and Communications Association committee. The committee investigated the issue and it resulted in the termination of Bell Pottinger's membership with the body for discrediting the industry (Central, 2017; Testa, 2018; Withers, 2017:1). While Bell Pottinger's reputation has been tainted, the main impact of the campaign was on South Africa and its people. The outcome of this campaign was an increase in racial tension in South Africa, a country that has a history of such tension.

Another threat to the South African environment is the use of social media for criminal activities. In the main, the investigation of social media in the use of criminal activities is the

[54] The state capture report was compiled to "investigate complaints of alleged improper and unethical conduct by the president and other state functionaries relating to alleged improper relationships and involvement of the Gupta family in the removal and appointment of ministers and directors of state-owned entities resulting in improper and possibly corrupt award of state contracts and benefits to the Gupta family's business" (Public Protector South Africa, 2016:4).

responsibility of the South African Police Service (SAPS) according to the mandate set out in the Constitution of the Republic of South Africa (1996:105). Specific units within the SAPS such as the Department of Priority Crime Investigations (DPCI) apply SOCMINT during their investigations (Turck, 2016:130). These investigations include finding missing persons, finding suspects and the investigation of criminal activities (Turck, 2016:130).

This section emphasised how social media application in South Africa can pose treats to its national security. Even though SOCMINT is currently being used within the intelligence agencies, it is not used to its full potential, especially in the SSA (civilian intelligence) environment. In order to raise the level of application within the intelligence environment, a strategic framework is needed to guide the process. The next section compiles such a strategic framework to include SOCMINT in the intelligence environment.

8.4 Incorporating SOCMINT into the intelligence framework – a new intelligence framework for the South African context

The new global environment has necessitated a new look at intelligence and intelligence organisations to improve efficiency. Walsh (2014:132–134) studied the intelligence frameworks of the "Five Eyes/5 Eyes"[55] and came up with an outline of what is needed in the new information age to keep intelligence communities relevant. The outline is as follows:

- A clear intelligence doctrine to set out common policies and procedures: Such a doctrine, applicable to the entire intelligence community, will govern intelligence activities and actions. This will limit ambiguity, as the community will be guided by the collective policies and procedures.
- Flexibility of the doctrine: This is of great importance in cases where there has to be cooperation between national and international agencies. Inflexibility should not stand in the way of cooperation between agencies.
- Training requirements of personnel: Even though intelligence training has always been high on the agenda of most intelligence agencies, the focus was more on intelligence issues. The global landscape has changed and intelligence training should be reconsidered. Broader training is needed, especially with regard to technology and its applications.

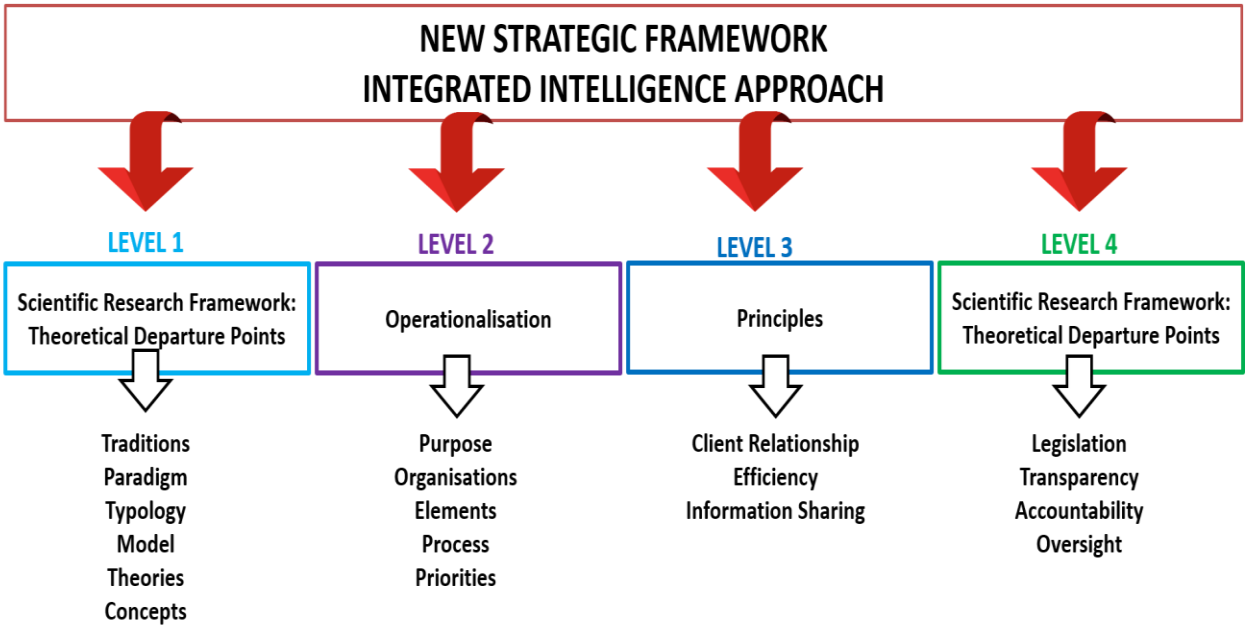
[55] Australia, Canada, New Zealand, the UK and the USA.

- The latest ICTs: Most intelligence agencies are using old communication technologies. The reason for this varies from budgetary constraints to the lengthy procurement processes within government.
- Leadership: It is of great importance to have leadership that understands the intelligence environment (Walsh, 2014:132–134).

The main aim of the new strategic framework for South Africa is to include SOCMINT at all levels of intelligence. Furthermore, the framework also focuses on various issues that have to be considered to address new challenges, increase efficiency and attend to the important issue of transparency.

The proposed strategic framework has four levels (Figure 58):

- Scientific research framework: theoretical departure points.
- Operationalisation: intelligence purpose; intelligence organisations; intelligence elements; intelligence process, sources and tools; and intelligence priorities.
- Principles guiding intelligence.
- Governance: legislation, transparency, accountability and oversight.



Source: Own construct

Figure 58: Outline for new strategic framework

The first level of the framework is the theoretical point of departure that is discussed in the section below.

8.4.1 Scientific research framework: theoretical points of departure

The strategic framework is grounded in the theoretical departure points discussed in previous chapters (Chapters 2, 3 & 4). These points provide the theoretical basis for understanding the proposed framework. The first aspect of the theoretical basis is tradition (Chapter 2). Traditions play a key role in guiding the researcher in terms of the historical perspectives in the particular academic field. With respect to intelligence, the traditions that were identified include the security environment, secrecy, surveillance and the intelligence cycle.

The second theoretical aspect is the paradigm. Chapter 2 determined that a new paradigm is needed for intelligence in the post-Cold War period. Furthermore, an interactive and interconnected paradigm would be more applicable to intelligence in the information age.

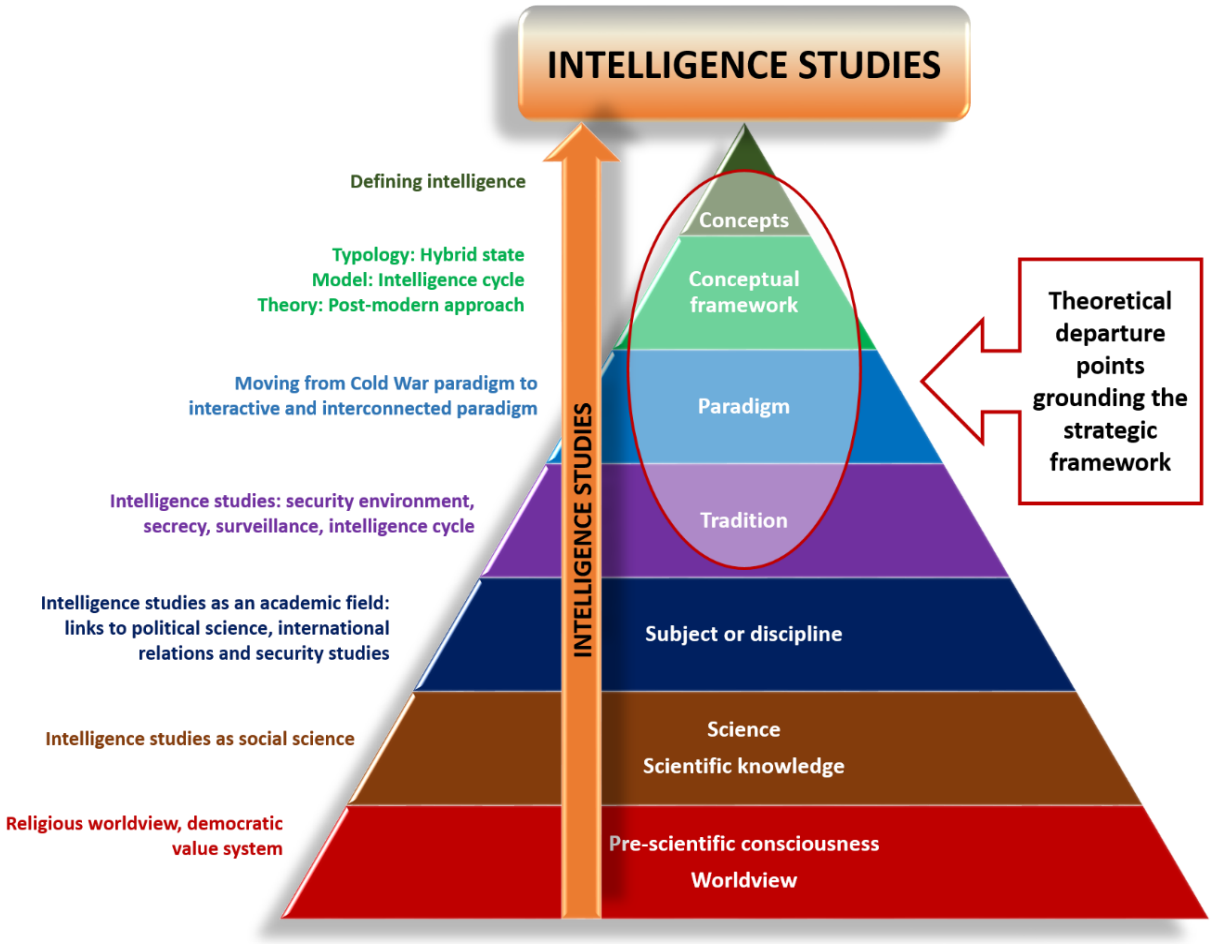
The next feature of the theoretical base is the conceptual frameworks. Three conceptual frameworks are of importance to this study: typology, models and theories (Chapter 2). With regard to typology, South Africa can be classified as a hybrid state. This classification implies that the civilian intelligence service is less democratic, more politicised and less accountable. This classification has far-reaching implications for the intelligence community's objectiveness. On the matter of models, the intelligence cycle was discussed at length and it was concluded that the cycle is not the correct way to describe the intelligence process. A better way to conceptualise the intelligence process would be a multi-layered linear model. This model allows for feedback at any stage of the intelligence process. The final conceptual framework is theories. Chapter 3 concluded that post-modernism offers a reliable alternative to realism for understanding intelligence in the post-Cold War era. Some of the characteristics that are especially relevant to the social media era include knowledge economy, uncertain identity, blurred state boundaries and the end of the intelligence factory (Rathmell, 2002:95–98). An important characteristic of post-modernism is what Rathmell (2002:98) specifies as the "end of the intelligence factory". This refers to the impact of technology development on the way business is being conducted. This characteristic can also be applied to the intelligence cycle and implies two issues. The first is that the intelligence process (which can be compared to the process in a factory) can no longer be described in a cyclical fashion. A new description for the intelligence process is needed. It

also refers to the fact that intelligence organisations are no longer the sole producers of intelligence. The current global information era can be characterised as a knowledge economy. The computer, together with the internet and mobile phones, has created an economy driven by the commodity of knowledge and information. The government, the private sector, individuals and non-governmental organisations are competing to produce or access the best information. The group or individual who wants to win this race needs access to current ICT and skills. The intelligence community is competing in this arena.

The final aspect of the theoretical base is concepts, particularly the concept of intelligence (Chapter 3). For the purposes of this study intelligence is defined as:

- The collection of information pertaining to all threats and opportunities from all available sources.
- The analysis, integration and interpretation of information into a product.
- The timeous dissemination of the final product to the national client to assist in policy decisions.

The summary of this discussion is depicted in Figure 59 below. The conceptual framework of intelligence that was constructed in Chapter 3 is used as the basis for the discussion above. The components that are applicable and form the theoretical base for the new strategic intelligence framework are the traditions, paradigm, conceptual frameworks and concepts.



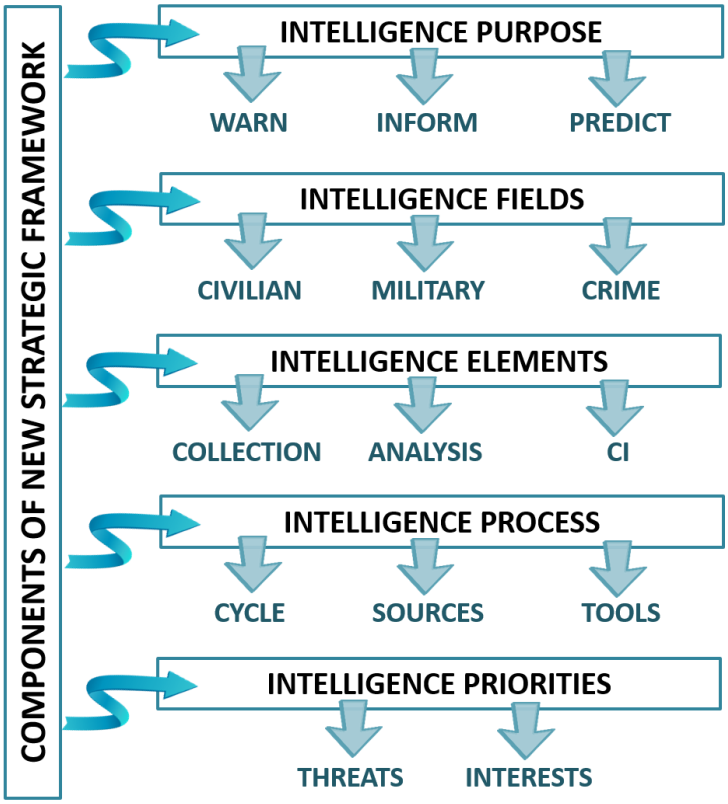
Source: Adapted from Duvenhage, 1994:60; Greffrath, 2015:29

Figure 59: Theoretical departure points: new strategic framework

With these theoretical points of departure as basis, the next section of this chapter focuses on the components of the new strategic framework.

8.4.2 Second level: Operationalisation

The main objective of this new framework is to incorporate SOCMINT as a new source of information into the national security environment. This study has identified five components that are of importance in the operationalisation of the new strategic framework. These components include intelligence purpose, intelligence fields, intelligence elements, intelligence process and intelligence priorities (Figure 60).



Source: Own construct

Figure 60: Operational level of strategic framework

A detailed discussion of these components follows.

8.4.2.1 Intelligence purpose

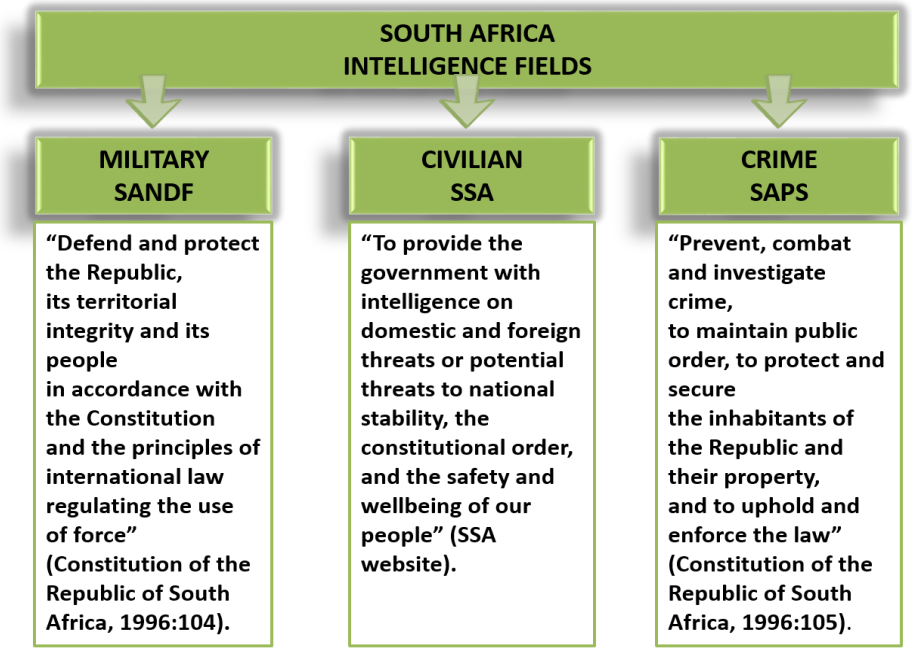
It is imperative to highlight the purpose and functions of intelligence as these guide and mandate intelligence organisations (Repeated Figure 39). Chapter 5 concluded that intelligence has three primary functions: to warn the policy maker about threats to and opportunities for national security; to inform the policy maker about new trends that might affect national security; and to predict future threats and opportunities.

Source: Adapted from Classen 2005

Repeated Figure 39: Primary purpose and functions of intelligence

8.4.2.2 Intelligence fields

The intelligence fields and the responsible departments are depicted in Figure 61 below. The intelligence fields include the military, civilians and crime. These fields are discussed in more detail in Section 8.5.



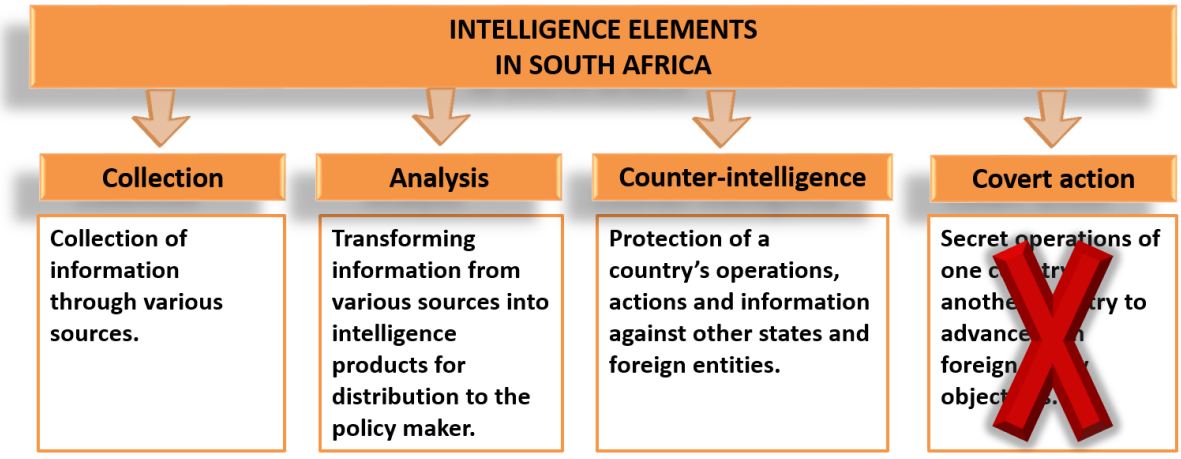
Source: Own construct

Figure 61: Intelligence fields in the South African intelligence environment

With the intelligence field clarified, it is important to discuss the intelligence elements of the operationalisation level.

8.4.2.3 Intelligence elements

Intelligence elements consist of collection, analysis, CI and covert action (see Chapter 5, Section 5.3). In the case of South Africa, covert action is illegal in terms of the White Paper on Intelligence (1995:7). Figure 62 below depicts the elements within the South African environment. These elements include collection, analysis and CI.



Source: Own construct)

Figure 62: Intelligence elements

The next component of the operationalisation level is the intelligence process, which is discussed in detail below.

8.4.2.4 Intelligence process

Perhaps the most important component of the new strategic framework is the intelligence process, as the inclusion of SOCMINT will affect this aspect the most. The issues that are addressed in this section include the intelligence cycle (multi-layered model), sources and tools.

Multi-layered model of intelligence

As mentioned previously, the intelligence cycle was identified as one of the traditions of intelligence (Chapter 2). However, scholars and practitioners have come to realise that the intelligence cycle does not sufficiently address the current intelligence process or challenges

facing the intelligence community (Clark, 2013:5; Gill & Phythian, 2006:3; Hulnick, 2006:959; Lowenthal, 2006:66). Berkowitz (1997:112) is of the view that the intelligence cycle is too bureaucratic and was appropriate for the 1940s and the 1950s and should change to accommodate the new security environment. This is in line with the argument highlighted in this study that a new strategic framework is needed to include new threats and sources of information resulting from communication technologies.

Some of the problems with the intelligence cycle include the following:

- Driver of the intelligence process: The driver of the intelligence process is no longer the direction provided by the client (government), but the gaps in the intelligence picture (Hulnick, 2006:959). The intelligence community is self-driven, as these gaps are identified internally by analysis. These gaps in the information are then provided to collection for further investigation.
- Feedback: The most common issue with the cycle is that it does not sufficiently allow for the feedback process (Berkowitz, 1997:112; Gill & Phythian, 2006:3; Lowenthal, 2006:66). This includes feedback from the client and internally from analysis to collection.
- Intelligence elements: CI and covert action is not part of the intelligence process (Hulnick, 2006:959).
- Sharing of information: Each activity works in isolation and does not share information (Clark, 2013:7–8). This leads to an incomplete product that will have a negative impact on the policy making process.
- Technological development: Intelligence organisations do not keep up with changes in technology developments. During the early stages of technology development, it was the government who led innovations (Berkowitz, 1997:109). However, this situation has changed and currently the private sector is outpacing the government when it comes to innovations and new technology development (Berkowitz, 1997:109).

In order to address the above-mentioned problems this study is proposing a new model of the intelligence process (Figure 63). This new process is multi-layered with three elements: analysis, collection (internal and external) and CI. The intelligence process is driven by two actions: by the client through the delineation of requirements and by the internal tasking generated as a result of gaps in the information. The traditional intelligence process/cycle has four elements: collection, analysis, CI and covert action. As mentioned previously, covert

action is a controversial issue and in the case of South Africa it is illegal. It is therefore not included in the new model.

The relationship between the policy maker and the intelligence organisation is a complex one. Even though the process usually begins with requirements or requests form the policy maker, this is not always the case. In most cases the requirements are self-generated within the organisation, guided by the priorities as set out in the National Intelligence Priorities (NIPs) and the NIE. In some cases the requirements are not clear and the intelligence organisation does not have the opportunity to interact with the policy maker to clear up uncertainties.

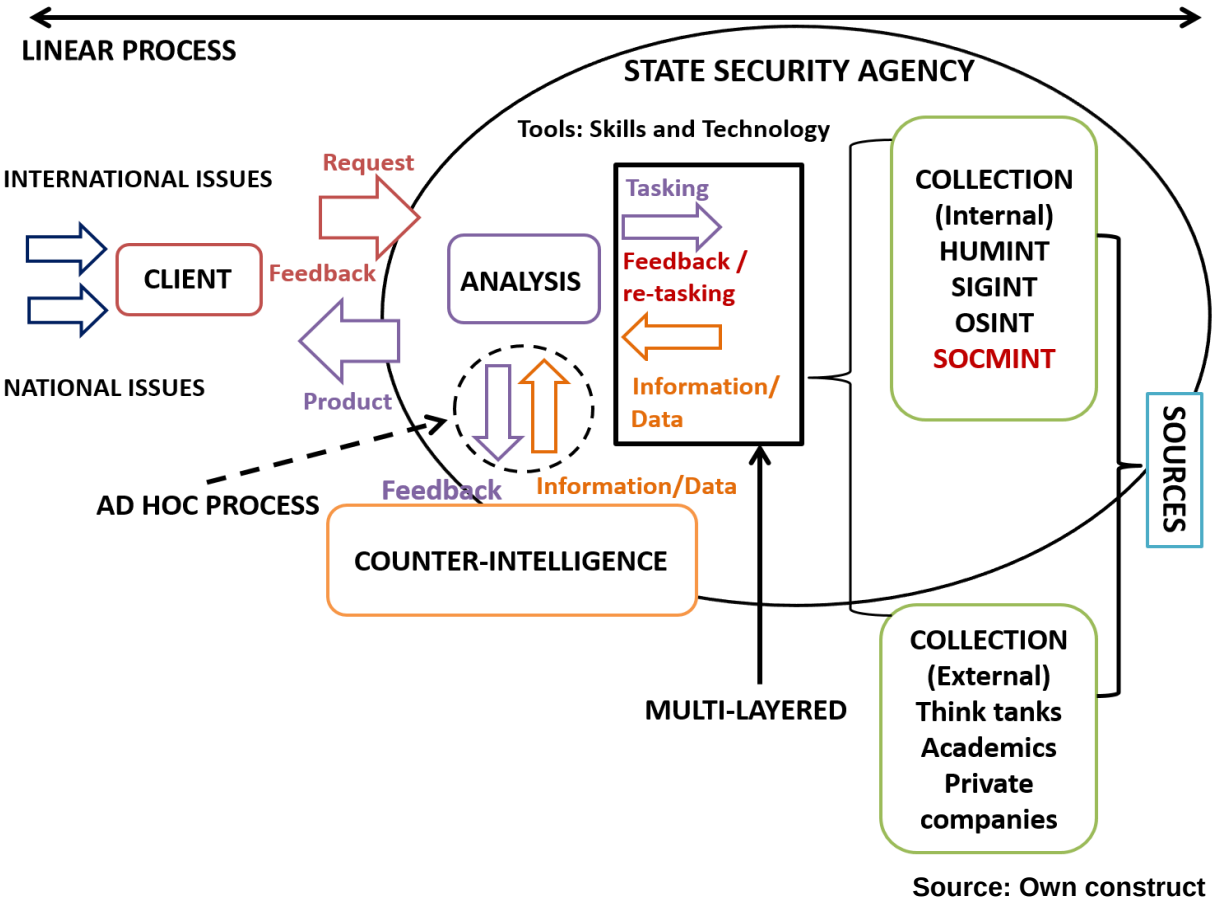


Figure 63: New Intelligence process, sources and tools

The first element of the model is analysis (see Section 5.3.2). Analysis is placed at the centre of this process as this study views it as the most important element and driver of the process. Within the intelligence community, the priorities and requirements received from the client are communicated to analysis. These are then critically examined to compile requirements and provide direction to the collection arms. Analysis has access to all available information and is in a position to determine the gaps. The requirements are then

distributed to the collection arms of the intelligence organisation. Analysis can also provide recommendations to determine the type of sources to be applied. Information collected through the collection arms are sent back to the analysis arm for processing. The processing entails the evaluation of the information, collation of all relevant data, analysing and finally dissemination to the client. An important aspect of analysis is feedback. After receiving the information from the collection arms, the analysis division must provide feedback on the relevance and usefulness of the information to the collection arms. If there are still gaps, a new requirement is compiled and distributed. This activity of feedback and re-tasking is the multi-layered aspect of this new process.

The second element of the process is collection (see Section 5.3.1). Collection is divided into two sections: internal and external. The internal process is managed by the various collection arms within the intelligence community. These collection arms include human sources (HUMINT), interceptions of communication between two entities (SIGINT), open sources (OSINT) and social media (SOCMINT). These collection arms receive the tasking from the analysis division. The relevant information is collected and channelled back to the analysis component. The second part of collection is the external collection capability. With the new security environment, new skills are needed, especially related to technology and its applications. These skills are not always available within the intelligence environment. If the intelligence organisation wishes to remain the provider of choice, it will have to outsource capabilities not available within the organisation. These skills can be acquired through recruiting and training or the acquisition of computer programmes. However, intelligence organisations do not always have the financial means. Some of these skills or computer programmes that can be outsourced are related to issues such as social media mining and the analysis of the social media data. The information obtained from the external sources will feed directly into the analysis process and will be handled in the same way as the internal collection process. This information will also be evaluated, collated and analysed before feedback is provided regarding the usefulness and application.

The third and final element of this process is CI (see Section 5.3.3). This element was not included in the traditional intelligence cycle. For the purposes of this study, CI is included in the new model within the domain of the intelligence community and within the national borders of South Africa. As mentioned in Chapter 5, CI includes the offensive and defensive actions undertaken to safeguard the entire intelligence process against operations and actions from foreign entities (governments, private companies and individuals). As CI is a specialised area of intelligence, it has its own collection and analysis capabilities. Although most of the information collected by this structure is not relevant to the rest of the intelligence

process, applicable information can be shared (on an ad hoc basis) with analysis to complete the intelligence picture.

In the introduction it was mentioned that the main aim of the new framework is to incorporate SOCMINT on all levels of intelligence. In this regard it is imperative to indicate how SOCMINT will feature within abovementioned elements of the new model of the intelligence process (Table 8). To accommodate SOCMINT, new structures with social media and technical skills are imperative. During analysis, the information and data received from the internal and external social media collection processes will be included in the compilation of products. In order to analyse social media data, there should be a unit of analysts with the skills to scrutinise and interpret the data. Internal collection will have to establish a SOCMINT collection unit. This unit will need the necessary technical skills and computer programmes to collect relevant information. The information collected will be sent to analysis and CI. The CI analysts will evaluate the data from a CI perspective.

Table 8: SOCMINT structures within the intelligence process

ELEMENTS	ACTIONS	SOCMINT STRUCTURES
Analysis	Scrutinise and interpret social media data	Analysts with the necessary analytical skills to work through data and interpret the social media information
Collection	Collect social media data with computer programs	Personnel with technical skills to operate the programs and to obtain the relevant data
Counter-intelligence	Scrutinise and interpret the social media data	Analysts with the skills to work through data and interpret the social media information as it is relevant to the CI environment

Source: Own construct

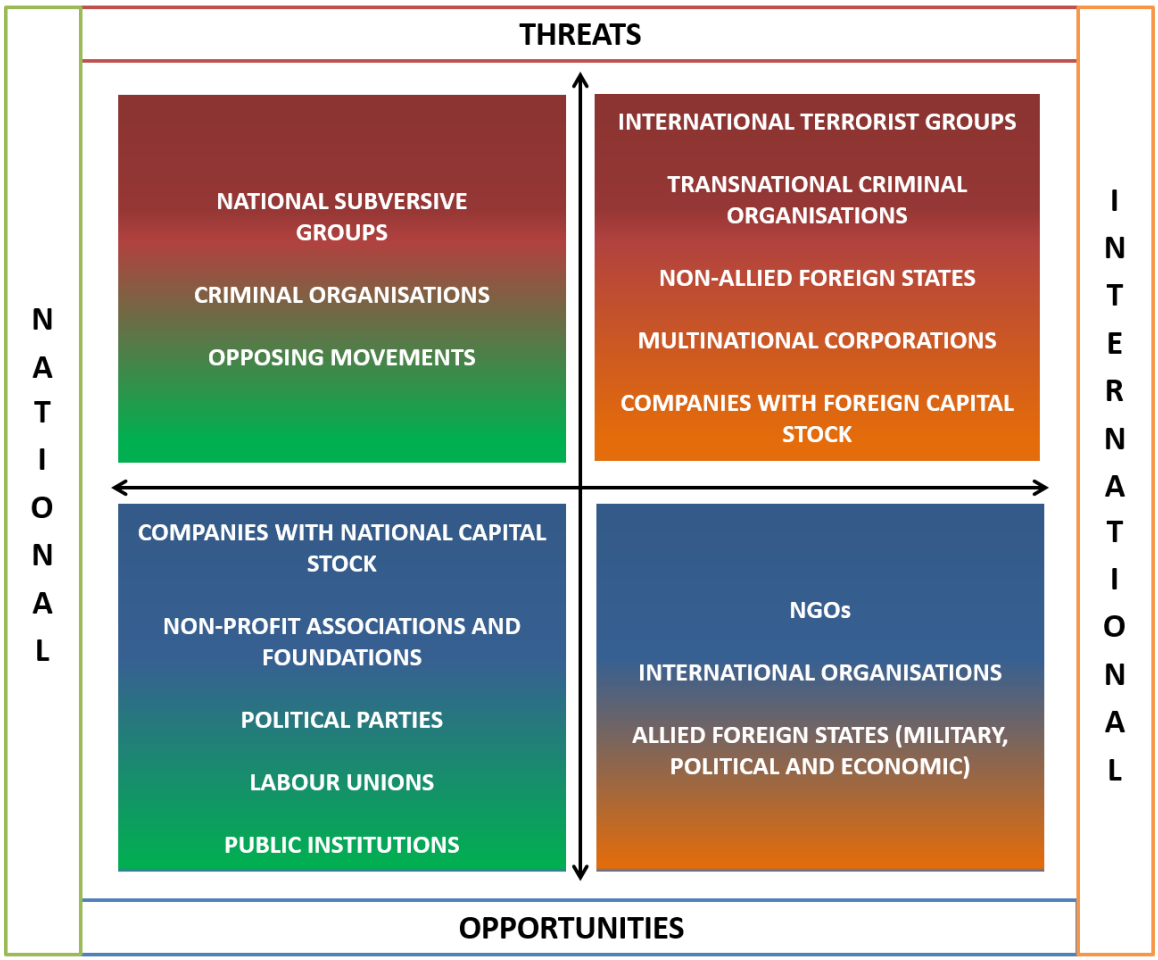
The next element related to the intelligence process is sources, which is discussed below.

Sources of information

With the proposed intelligence process clarified, it is important to look into the sources of information. An intelligence organisation cannot survive without sources of information. In order to remain relevant, intelligence organisations and their source bases have to grow and change as technology and the security environment change. As mentioned in Chapter 5, most intelligence organisations classify sources of information as technical intelligence, HUMINT and OSINT. The technical intelligence includes signals, imagery and MASINT.

These classifications of sources do not make reference to the latest technological intelligence source, SOCMINT.

SOCMINT is the latest addition to the source database of intelligence organisations. Most intelligence organisations have not yet included this important source of information as part of their intelligence framework. Social media can both be viewed as a threat to and an opportunity for national security. The application of social media to organise and mobilise users for protests is viewed as a threat to national security (for a detailed discussion on SOCMINT, see Chapter 7). However, the information on the social media platforms can serve as an opportunity to get information. It is therefore important to identify the organisations or groups that could use social media within the borders of the country and internationally and to classify them as threats or opportunities. This will provide the intelligence organisations with a broad framework to identify the areas where resources should be focused to obtain information from social media. Figure 64 depicts this situation. The figure represents social media as a threat and opportunity on a national (domestic) and international level. National groups that are viewed as threats include national subversive groups, criminal organisations and opposition movements (Montagnese, 2012:12). National groups that could provide opportunities to counter threats and protect national interests include companies with national capital stock, non-profit associations, political parties, labour unions and public institutions (Montagnese, 2012:12). International terrorist groups, transnational criminal organisations, non-allied foreign states, multinational corporations and companies with foreign capital stock are viewed as threats to national security from an international perspective (Montagnese, 2012:12). On the other hand, NGOs, international organisations and allied foreign states are viewed as opportunities to national security (Montagnese, 2012:12).



Source: Adapted from Montagnese, 2012:12

Figure 64: Organisations: posing threats or providing opportunities

With this discussion of sources as background, it is important to consider the tools needed for the intelligence process. These tools include skills and technology and will be discussed below.

Tools in the intelligence process

In the previous section the importance of sources was underlined. However, human resources (personnel) within the intelligence organisation are equally important. Without the collection of relevant information and the compilation of useful products, the intelligence organisation will not be able to make a contribution to the policy making process. The changes in the global security situation and the new threat environment since the end of the Cold War have particular implications for the required skills needed within the intelligence organisation (Agrell, 2012:131). Relevant and useful products are reliant on employees with applicable skills in collection tradecraft and analysis. Traditionally and before the information age, the collection and analysis were the most important skills within the intelligence

organisation. Though, as communication technology expanded, the need for technical skills and expertise increased and became just as important to the success of the intelligence organisation.

Previously, the intelligence environment was one-dimensional, with skills limited to analysis and collection. However, with the development of communication technologies the environment has changed and has become so complex the expertise within the organisations is not sufficient. New threats require new skills. In order to increase the relevant skills in the intelligence organisation, a strategy of recruitment and training is needed. The new intelligence process discussed above emphasises the collection and interpretation of data from social media sources. This calls for a recruitment strategy aimed at experts in social media, both on the collection and analysis side.

The second important tool necessary to perform the critical functions of intelligence organisations is technology. Technology is currently the driver of the global environment. If intelligence organisations are to develop and remain relevant they have to acquire and apply the latest communication technologies (Tenet, 2010:136). This implies that to remain pertinent, intelligence organisations have to implement and use the latest technologies to provide an intelligence product that is current, reliable and effective. If intelligence communities do not change and implement new technologies, they run the risk of falling behind and becoming irrelevant. Not only should the intelligence organisations have the latest technologies, they also have to understand the technologies and the threat to national security (World Economic Forum, 2017:43).

Technologies that are of importance to the intelligence community include the following:

- Secure communication technologies to communicate with sources.
- Computer programs to collect and analyse information from social media platforms.
- Computer programs to assist with analysis and make predictions.
- Secure communication technologies to communicate with the client.
- The latest computer models to increase efficiency.
- Quick internet connections to increase efficiency.
- Surveillance technologies.

With this discussion of the intelligence process as background, it is equally important to discuss intelligence priorities.

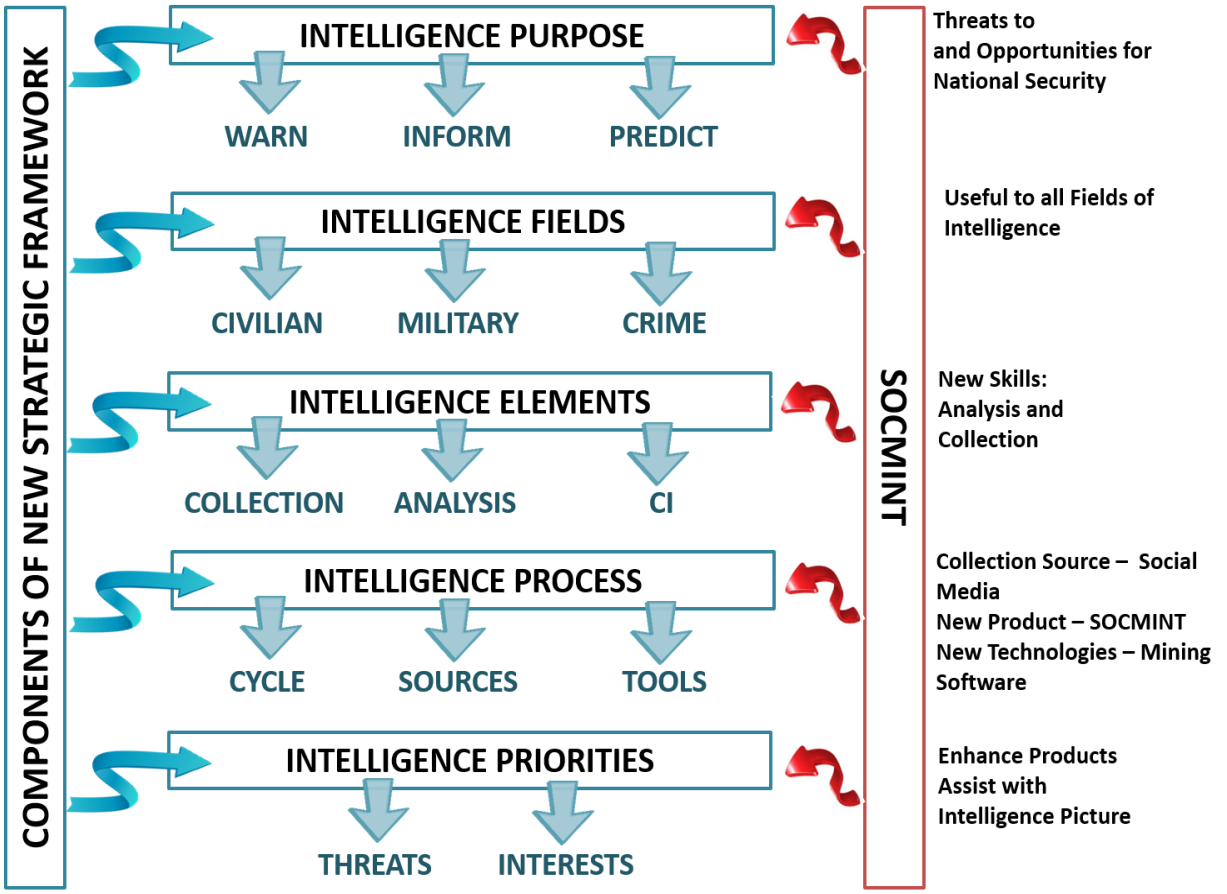
8.4.2.5 Intelligence priorities

What is expected of the intelligence community in the 21st century? The expectations have not changed, they have remained the same throughout the ages. According to Classen (2005:73), these expectations include the following:

- Intelligence organisations have to provide objective intelligence to the policy maker to either endorse or amend current policy direction.
- Intelligence organisations have to provide intelligence on potential threats. These are issues that have the potential to become a problem in the future.
- Intelligence organisations have to respond to requests from the national client and other government departments as the need arise.

Within the South African environment, the priorities for the intelligence community are set out in the NIE. The NIE is compiled by NICOC based on input from the SSA, Crime Intelligence (SAPS) and the ID (SANDF). After approval by the cabinet, the NIE serves as a guideline for the intelligence process (collection and analysis).

This discussion on the operational level of the framework and the inclusion of SOCMINT as part of each component are depicted in Figure 65 below. Within each component, SOCMINT plays a key role. With regard to the purpose, SOCMINT assists in identifying threats and opportunities. SOCMINT can be used in each of the fields of intelligence: military, criminal and civilian. New skills are needed in areas of analysis and collection to extract relevant information and to reach the correct conclusion. SOCMINT is a new source of information. Furthermore, it can also be viewed as a product on its own or as a product that can enhance other products. New technologies such as mining software are needed as tools to extract the information. In general, SOCMINT can enhance products to create a clearer intelligence picture.



Source: Own construct

Figure 65: Operational level of strategic framework and SOCMINT

This section discussed the second level of the new strategic framework for intelligence. The next segment addresses various principles that are of importance for intelligence organisations to be successful. Principles such as client relations, information sharing and efficiency help intelligence organisations with their tasks.

8.4.3 Principles of the new intelligence framework

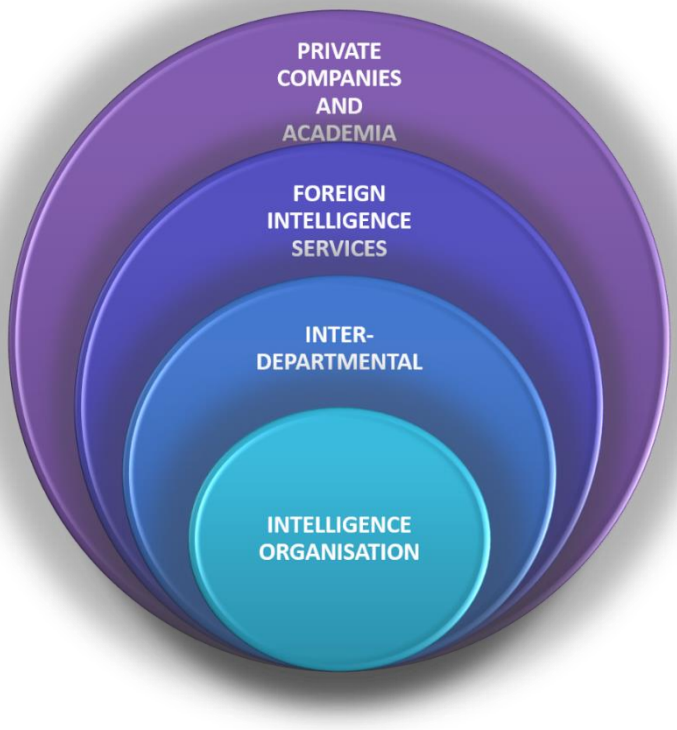
Intelligence organisations should follow certain principles for the framework to be successful. These principles include the following:

- Client relationship: The client and intelligence organisation relationship is important for the success of an intelligence organisation. Although a close relationship between the intelligence officer (analyst) and the client is not preferable (policy bias), it could help with trust between the two parties (Dupont, 2003:24–25). Furthermore, it can assist the

intelligence officer in better understanding the decision-making and policy process, which could enhance analysis of the issue. The timely delivery of relevant and accurate information is made difficult by the access to and distribution of information by a wide range of individuals with access to the internet and cell phones. In today's environment it is all the more important to have specific requirements from the client and to know exactly what the client expects of the intelligence community (Clift, 2008:1).

- Information sharing (coordination and cooperation): Information sharing is an important debate within the intelligence community and has been highlighted after the 9/11 attacks. In this case information sharing was an important reason for intelligence failure (Kruys, 2006:72; Lawless, 2012:1). The interconnectedness of the global world is the outcome of communication technology, which has resulted in, among other things, the social media phenomenon. As a result of the changed global security environment, Chapter 2 found that intelligence needs a new paradigm. The interactive and interconnected paradigm was mentioned and discussed. This paradigm focuses on the global exchange of intelligence necessitated by the current borderless environment. This view is in line with Berkowitz (1997:107), who is of the opinion that the information revolution necessitates reforms within intelligence organisations, with information sharing as an important aspect. Although Campbell (2013:62–63) also highlights the issue of information sharing, he cautions that it has positive and negative consequences; positive in the sense that it assists with creating the bigger picture, negative in that information is available to a wider range of people and this could compromise operations and sources. The issue of information sharing was highlighted in Chapter 3 (Section 3.2.2) as an important part of diplomatic engagement between intelligence services. Information sharing among intelligence services is an important factor to address the new borderless security environment with its cross-border threats. The availability of intelligence should be borderless and the only way to accomplish this is to have information sharing agreements between intelligence services. Taking all these views into account, the author proposes that the principle of information sharing must be addressed in four layers (Figure 66): within the intelligence organisation, interdepartmental (nationally), among intelligence organisations (internationally) and with private companies, individuals and academia (national and international). The first layer of sharing is within the intelligence organisation. Departments within the intelligence organisation should not work in silos and all information should be channelled to the analysis arm. The second layer is interdepartmental information sharing. Relevant information should be communicated to departments within government to assist with decision-making and policy issues. The third layer of information sharing is among foreign intelligence services. New global threats do not adhere to the sovereignty and borders of countries. It

is therefore imperative for intelligence organisations to share intelligence to remove or at least minimise the impact of these threats. SOCMINT is an important source of information that will enhance the intelligence picture and products to be shared with the intelligence organisations of allied countries. The final layer is that of the private sector and academia. This relationship will be less sharing and more receiving information. This could increase the analytical depth of products and provide other perspectives on issues.



Source: Own construct

Figure 66: Information sharing model

- Efficiency: The future of intelligence is dependent on how well the intelligence community adapts to the new security challenges in general and the information revolution in particular. A crucial challenge the intelligence community has to deal with is that the ICT revolution has increased the pool of intelligence producers. One of the most important issues for survival is efficiency. This is especially important with the competition from non-governmental intelligence organisations. Goodman and Berkowitz (2008:313) suggest that to be efficient, the intelligence organisation should in the first place pay attention to planning and allocation of resources. The path from collection to analysis and dissemination should be as short as possible. This is especially true in the current communication technology age where the internet and computer technologies have made time and distance obsolete. A second and important issue is to maintain the

integrity of analysis (Goodman & Berkowitz, 2008:317). This can only be realised if the intelligence organisation remains objective and does not become politicised.

The next and final level of the new framework relates to governance issues and provides the environment for intelligence organisations to perform their tasks and functions within the boundaries of a democratic value system.

8.4.4 Governance (legislation, transparency, accountability and oversight)

An important feature of this new strategic intelligence framework is the legal outline that governs the intelligence process with regard to transparency, accountability and oversight. The issue of oversight within intelligence organisations has gained attention over the past 20 years, especially after the intelligence failure of the 9/11 attack (Omand & Phythian, 2012:28). Before 9/11, especially during the Cold War period, intelligence organisations were free from scrutiny because of the secrecy. Democracy requires oversight, but intelligence organisations conduct business in secrecy. There is a need for a balance between transparency and secrecy. The South African White Paper on Intelligence (1995:4) also underlines this principle of "the balance between secrecy and transparency".

Secrecy is a necessary feature of an intelligence organisation for the following reasons:

- Targets should not be aware that they are under surveillance.
- Methods used by services should not be made public.
- The identities of sources and operatives have to be protected.
- The information received from foreign services has to be protected.
- The intelligence organisation should avoid being compromised by rival intelligence services (Nathan, 2012b:51).

While secrecy is necessary, there is a need for transparency, accountability and oversight, especially in relation to democracies. Various mechanisms and pieces of legislation have been implemented in South Africa to assist with the issue of governance. However, the social media phenomenon has not been addressed in a direct way.

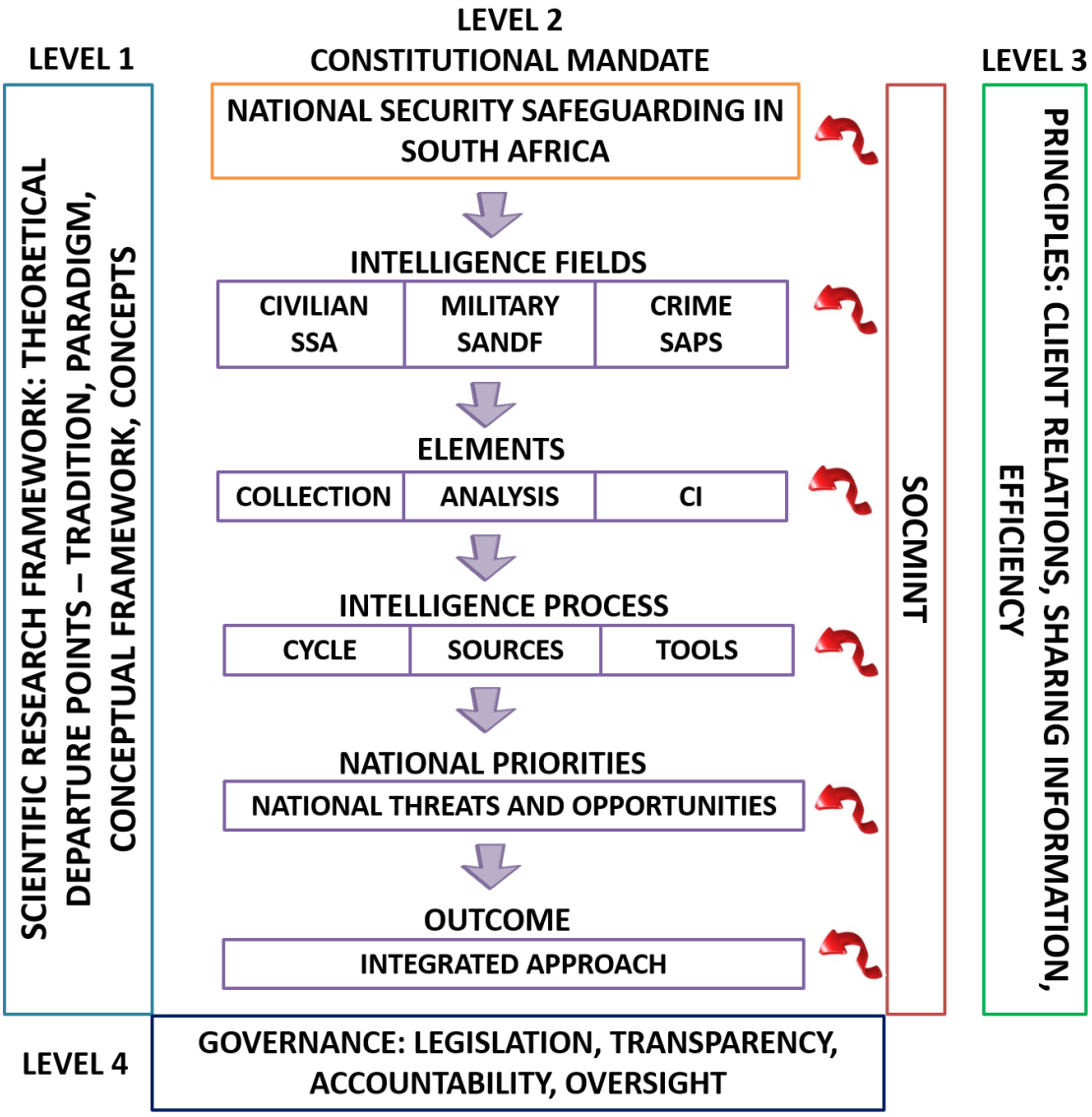
The intelligence community does have an obligation to utilise the social media platforms responsibly and legislation can assist. Omand *et al*. (2012a:11) proposes the following principles for SOCMINT collection and surveillance:

- Sufficient and sustainable cause: This principle will force intelligence organisations and law enforcement agencies to provide legitimate reasons for the surveillance. Some of these reasons include in the interest of national security, preventing or detecting crime or in the interest of public safety.
- Integrity of motive: The motive and reason why the information is needed should be clearly stated.
- Methods used proportionate and necessary: The degree of intrusion must be evaluated – the more intrusive, the higher the level of authorisation will be needed.
- Must be the right authority, validated by external oversight: The process must be well documented and must remain within the chain of command.
- Resorting to secret intelligence must be the last option if more open sources can be used: In relation to SOCMINT, less intrusive methods should be used if possible.
- Must be reasonable prospects for success: Operations in relation to SOCMINT should only be undertaken if there is a reasonable chance for success. In this case, success implies usable and actionable intelligence.

It is of great importance that the intelligence community adheres to legal practices to remain transparent and to respect democratic principles. However, this should also be in line with the secrecy fundamentals of the intelligence profession. These fundamentals relate to the protection of sources, methods and information.
With this detailed discussion on the levels of the new framework as basis, the next section summarises the new intelligence framework.

8.5 Summary: New intelligence framework

The above discussions culminate in the framework depicted in Figure 67.



Source: Own construct

Figure 67: Conceptualised integrated strategic intelligence framework for SOCMINT

The main aim of this new intelligence framework is to include SOCMINT at all the levels of intelligence. The framework is grounded in the purpose of intelligence. The key goal of this framework is to ensure that the intelligence organisation is the organisation of choice when it comes to intelligence. Furthermore, the framework consists of four levels. The first level is the scientific research framework that outlines the theoretical departure points. These departure points include traditions, paradigms, conceptual frameworks and concepts related to intelligence. The second level is the operationalisation of the components, such as the purpose, fields, elements, process and national priorities. The third level of the framework is principles and includes client relationship, information sharing and efficiency. The final level is governance and relates to legislation, accountability, transparency and oversight. A sound

legislative structure is of great importance, especially in relation to interception and use of social media information.

With this framework as background, it is imperative to discuss the findings of this study and to make recommendations with regard to the application of SOCMINT within the South African context. The next section focuses on these issues.

8.6 Findings and recommendations for the application of SOCMINT within the South African context

The previous section focussed on the development of a strategic framework for the application of SOCMINT within the South African context. This framework was developed on the basis of the findings from an in-depth literature study. The first part of this discussion concentrates on the main findings of this study.

8.6.1 Findings

The findings can be divided into two categories: findings applicable to the international context and findings directly related to the national context. Although the first category of findings is related to the international context, they also apply to the South African context.

8.6.1.1 Findings applicable to the international context

The following are findings pertinent to the international context:

Social media is a marketing tool that can also be used by intelligence organisations
Although social media analysis began as a marketing tool, the intelligence community soon realised that it could be applied in their line of work, especially to counter terrorism (Harrysson *et al*., 2012; Marshall, 2012). Marshall (2012) highlights that the USA's Homeland Security Department has been using this tool since 2009. However, as mentioned in Chapter 1, the term SOCMINT was only coined in 2012 by Omand *et al*. (2012a:804). Since then, the term has been used widely (Lombardi *et al*., 2016:1; Moe & Schweidel, 2014:1; Wright, 2013).

SOCMINT is being applied around the globe as part of the intelligence collection process. Israel is using the personal information posted on Facebook® to identify and recruit Palestinians to spy on Hamas (Donnison, 2010; Kubovich, 2016). In the same manner the

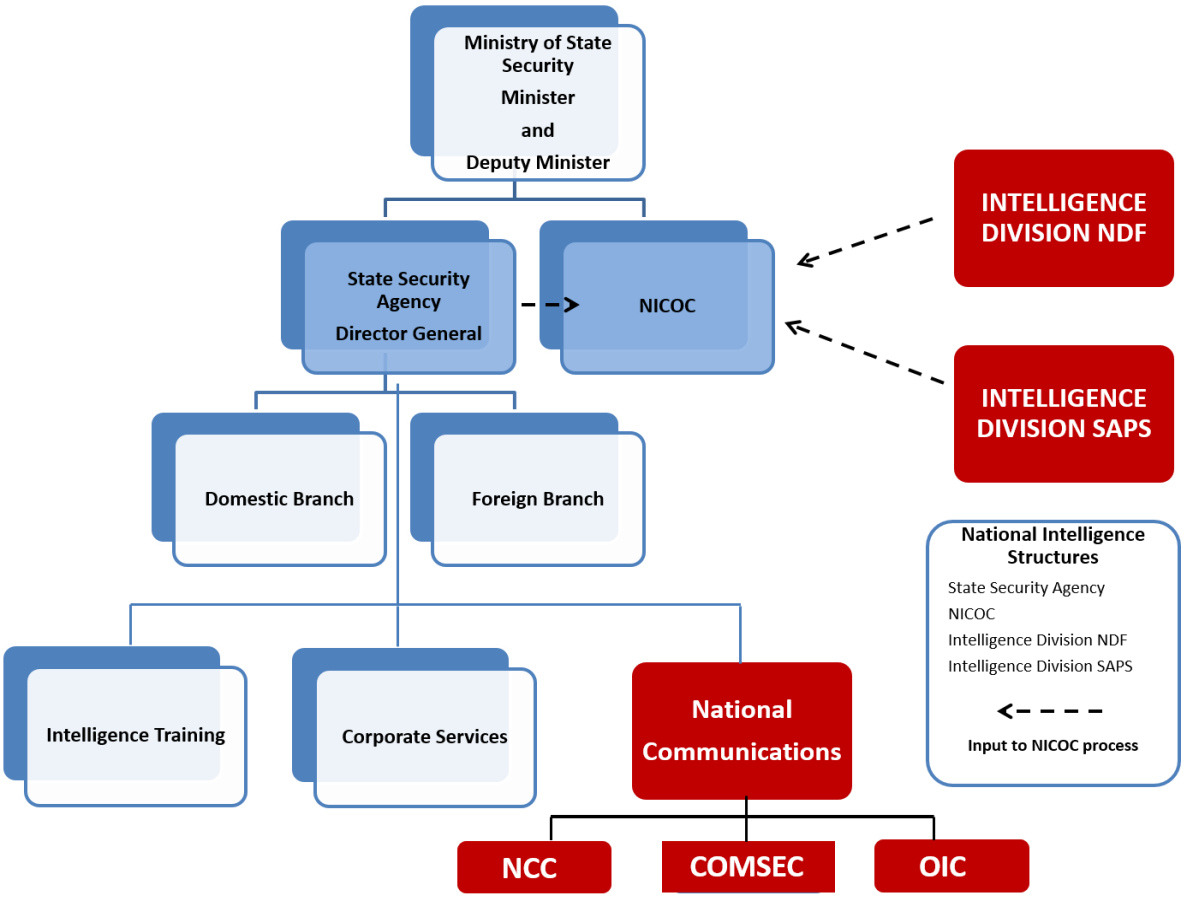
USA uses social media through fake accounts to influence and spread pro-American propaganda (Fielding & Cobain, 2011) and to collect data (Lang, 2017). The United Kingdom and Canada also collect information from social media sites to determine opinion and for law and other intelligence purposes (Briggs, 2017; Collins, 2015; Ismail, 2017; Ling, 2017; Rennie, 2013; Tannam, 2017). In most of the cases private companies are used to develop programmes that will help with the mining of information on social media using information already available in the public domain (Collins, 2015; Fielding & Cobain, 2011; Ling, 2017). While intelligence organisations are not forthcoming with the reasoning behind this practice, it might be because of a lack of expertise within these organisations. Furthermore, the private companies are continuously developing and upgrading software that offer their clients the latest technologies. As intelligence organisations are not in the computer business, they are not in the position to develop the software themselves.

The global trend of SOCMINT use is also established in South Africa. The intelligence agencies within South Africa use social media to collect information in line with their respective mandates (Swart, 2018; Turck, 2016:iii; Writer, 2014).

The first structure is that of the ID within the National Defence Force. The primary objective of the SANDF according to the Constitution of the Republic of South Africa (1996:104) is to "defend and protect the Republic, its territorial integrity and its people in accordance with the Constitution and the principles of international law regulating the use of force". The ID of the SANDF applies social media and the intelligence derived from it to assist with planning (Writer, 2014).

The second structure depicted in Figure 68 is the ID of the South African Police Service (SAPS). The Constitution of the Republic of South Africa (1996:105) states that the objective of SAPS is to "prevent, combat and investigate crime, to maintain public order, to protect and secure the inhabitants of the Republic and their property, and to uphold and enforce the law". Within the SAPS, the DPCI is responsible for the investigation of crimes related to the internet. According to the SAPS's 2010–2014 Strategic Plan (2010:9), the DPCI was established to "prevent, combat and investigate national priority offenses". The DPCI focuses on "serious economic crimes, with a key consideration being the combating of cybercrime and identity theft (focusing on securing the identity and status of citizens), corruption and organised crime" (SAPS, 2010:14). The final structure is the National Communications Branch, which reports to the Director General of the SSA. As per the SSA website, the mandate of the SSA is "to provide the government with intelligence on domestic and foreign threats or potential threats to national stability, the constitutional order, and the

safety and wellbeing of our people". Examples of such threats are terrorism, sabotage and subversion. This allows the government to implement policies to deal with potential threats and to better understand existing threats and improve their policies. The SSA website also indicates that the National Communication Branch consists of three components: the NCC, Electronic Communication Security (Pty) Ltd. (COMSEC) and the OIC. The RICA (70 of 2002) established the OIC, while COMSEC was transferred to the SSA according to Presidential Proclamation no 59 of 2009. The NCC is responsible for foreign signals interceptions. Figure 68 below depicts the intelligence structures in South Africa involved in surveillance, including social media surveillance.



Source: Adapted from SSA Website

Figure 68: Intelligence structures in South Africa

The application of SOCMINT means that the government should balance privacy, human rights and freedom of speech with national security

The monitoring or interception of social media by intelligence organisations across the globe has highlighted the issue of privacy, freedom of speech and national security (Mozaffari & Posno, 2016; Swart, 2011; Swart, 2017; Writer, 2018). This has placed intelligence

organisations in a difficult position. On the one hand the constitution allows for privacy and freedom of speech, while on the other hand the constitution tasks intelligence organisations with obtaining information for the purpose of national security (Figure 69). The intelligence organisations therefore have to balance privacy with issues of national security. In the case of South Africa, this task is being complicated by the lack of appropriate legal frameworks to deal with the issue of interceptions (Nathan, 2012a; Swart, 2016:3).

Source: Own construct

Figure 69: Intelligence organisations: Balancing act

On the matter of legality and social media monitoring, the Director General of the Office for Security and Counter-terrorism in the United Kingdom, Charles Farr, indicates that the monitoring of citizens on social media can take place without any warrant for interception because the service providers are not in the UK (Bowcott & Ball, 2014). However, the UK and the USA have various laws to govern the use of social media (see Turck, 2016:34–56 for a detailed discussion on these laws).

Various mechanisms and legislation have been implemented in South Africa to assist with the issue of governance. However, the social media phenomenon has not been addressed in a direct way. Even so, two acts are relevant and can be applied in this situation. The first act is RICA (70 of 2002). The RICA (South Africa, 2002d) regulates “interceptions of communications, monitoring of radio signals, radio frequency spectrums and the provision of certain communication related information”. This Act does not directly refer to social media (in 2002 social media was not an issue), but it can be inferred through the phrase

"interceptions of communications". The second part of legislation relevant to social media is the Cybercrime and Cybersecurity Bill. This Bill is in the process of being enacted and focuses on various crimes linked to cyber activities (South Africa, 2017:1).

Other South African laws that have implications for the monitoring and use of social media are the following:

- The Films and Publications Amendments Bill (B37B–2015) is currently before the National Council of Provinces and will regulate the distribution of online content (Davis, 2018).
- The Criminal Procedures Act (50 of 1977) regulates undercover operations. The Act is relevant if a false account for undercover operations is needed (Swart, 2018).
- The Protection of Personal Information Act (4 of 2013) relates to the storage and analyses of data (Swart, 2018).

In South Africa no warrant is needed to obtain personal information if it is in the public domain (Swart, 2018). However, according to the RICA (70 of 2002), it is illegal to intercept any communication not in the public domain without the permission of a judge designated to rule specifically on all interception applications in South Africa. Nevertheless, intelligence and law enforcement agencies in South Africa have used section 205 of the Criminal Procedures Act (51 of 1977) to circumvent the RICA process (Swart, 2011). The Criminal Procedures Act (51 of 1977) allows for the particular law enforcement or intelligence agency to apply to a high court judge, a regional court magistrate or a magistrate to grant access to cell phone records, telephone records or information about billing and ownership of a cell phone (Swart, 2011). Most of these requests come from SAPS and SSA (Swart, 2011). While the government's intelligence agencies deny the allegations of illegal interceptions, Swart (2011, 2015, 2017 & 2018) and the Right2Know Campaign[56] regularly report on illegal actions by these government agencies.

Increase in need for transparency and oversight

The intelligence organisations of the 21st century are increasingly faced with the challenges of oversight and transparency. Within a democratic government all actions have to be transparent as the government is accountable to the electorate (Dlomo, 2004:20). Intelligence has always sidestepped accountability and transparency because of the secret nature of its activities. However, this situation has changed as democracy increasingly

[56] According to their website (http://www.r2k.org.za/about/) the Right2Know Campaign is a movement that was launched in 2010 that focuses on freedom of expression and access to information.

requires transparency and oversight from intelligence communities (Dlomo, 2004:20). Governments and intelligence organisations themselves are gradually coming to understand the need for transparency and oversight. Nevertheless, there is a need to balance democracy and transparency when it comes to intelligence services.

New global intelligence environment

The environment where intelligence collection is taking place has changed from a predominantly physical world to a combination of the physical and cyber worlds. This has implications for both the intelligence collection and analysis process. With regard to the collection process, new sources must be identified and new methods of obtaining data should be implemented. Analysis on the other hand, is confronted with the increasing quantity of information, complicating the analysis process.

New threats to national security

The intelligence communities across the globe are faced with new threats to national security. At the time of the Cold War the intelligence doctrine was based on one threat: communism (Coyne *et al*., 2014:54). This doctrine provided the intelligence community with a clearly defined threat, with an unambiguous set of priorities that guided and provided some certainty to the intelligence process in general and analysis in particular (Coyne *et al*., 2014:53). However, with the end of the Cold War the nature of the threat changed and an increasing number of issues were included as threats to national security, creating uncertainty for the intelligence community. This did not imply that there were no threats, but it only meant that the intelligence communities were not equipped or prepared to attend to these threats (Lahneman, 2010:203). Non-traditional threats, as it was referred to during the Cold War, quickly came to the fore. These include transnational organised crime, terrorism, the proliferation of weapons of mass destruction, cybercrime targeting critical infrastructure and human security. This was also the start of the information age that was amplified by computer development. This new intelligence environment necessitated a new intelligence doctrine. However, the intelligence community continued to apply the Cold War doctrine of one threat to the new multiple threats security environment (Coyne *et al*., 2014:54). Since the new threats were not fully understood, it resulted in events such as 9/11 (Coyne *et al*., 2014:54).

The intelligence community is no longer the sole provider of intelligence as a result of communication technologies

The increased access to information as a result of information technologies has created competition with regard to the collection and provision of intelligence. This competition is on

two levels: first from actors outside of government (think tanks such as the Institute for Security Studies and South African Institute for International Affairs), which are increasingly generating intelligence products. The second level of competition is from new media. The new media technologies have created an environment where decisions and its implementation have to be made in real time (Andrus, 2005:1). This means that the intelligence–decision–implementation process is as short as 15 minutes (Andrus, 2005:1). The speed, volume and availability of social media have shortened the timespan of the intelligence–decision–implementation process. The internet and communication technologies have increased the supply of and access to information and knowledge. These technology advancements have created an "information based global society" (Degaut, 2016:509). This has eroded the information and knowledge advantage that was once the privilege of a small number of government intelligence institutions (Doorey, 2007:4; Dupont, 2003:33). The increase in the information supply will intensify the demand for timely and high quality strategic and operational intelligence. As communication technologies develop even further and reach more citizens across the globe, intelligence organisations will increasingly come under pressure to produce unique, secret, timely and useful information. In order to adhere to these requirements, the intelligence communities will have to adapt to new communication technologies. If not, the traditional intelligence community will lose its monopoly within the competitive knowledge environment (Agrell, 2012:131). It is of great importance that the intelligence community in South Africa fully adapt to new communication technologies. Andrus (2005:12) says that "We must transform the intelligence community into a community that dynamically reinvent itself by continuously learning and adapting as the national security environment changes." This study attempts to contribute to this process of reinvention and adapting.

Communication technology has blurred the lines between foreign and domestic issues

An important characteristic of the post-Cold War security environment and another challenge to the intelligence community, is that the lines between foreign and domestic issues have been distorted (Agrell, 2012:131), mainly as a result of communication technology development. These technologies have made it easier for criminals to move across borders without adhering to border control, blurring state boundaries. Threats can no longer be characterised as only domestic or only international. It is global security issues that impact on every nation. Snow (2014:2) refers to this as the "intermestic" dimension, where international and domestic influences intersect.

The next section focuses on findings that are specifically relevant to the South African context that impact on the intelligence environment.

8.6.1.2 Findings specific to the South African context

This study has revealed the following in relation to the South African context:

Unstructured use of SOCMINT within the intelligence environment

While information from social media is being used within the South African context, its application is not structured and issues such as a legal framework remain a problem.

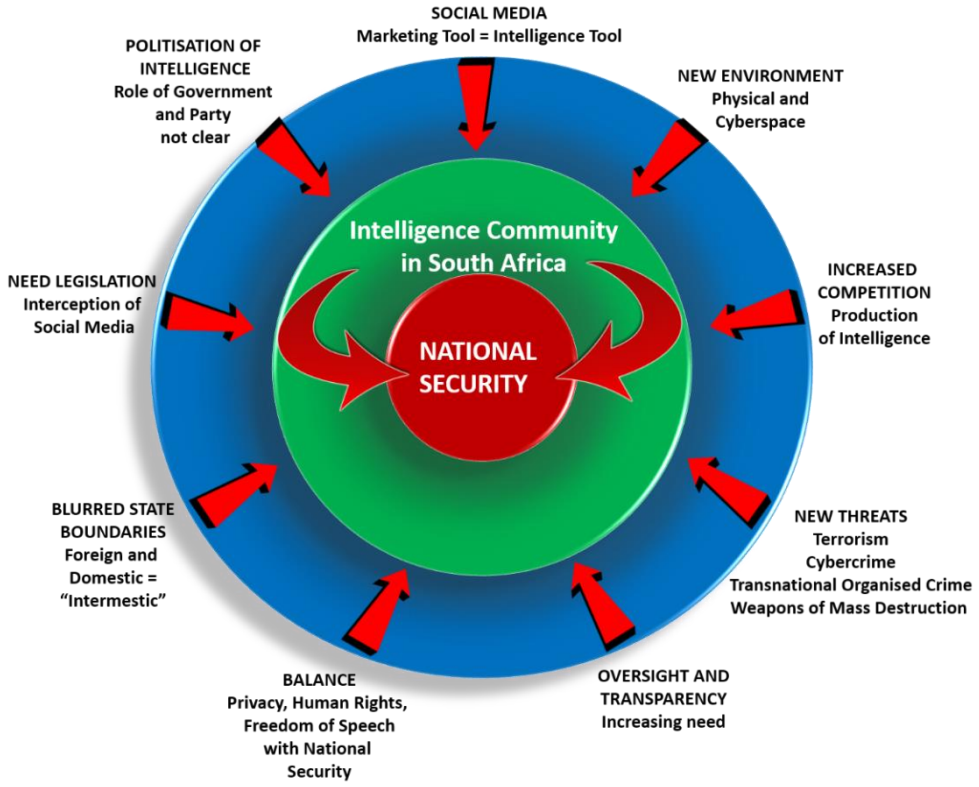
Politicisation of intelligence: Inability of the ANC to separate the role of the government and the party

South African government institutions in general and the civilian intelligence organisations in particular are currently faced with the inability of the ANC to separate the role of government and the party, affecting the policy making process and the service delivery of departments (Van den Berg, 2018:270). While the White Paper on Intelligence (1995:3) does indicate that security should be broader than military threats, the SSA has failed to adopt this approach in full. This has been especially true since former President Zuma came to power. During this time the SSA became highly politicised and the focus was on keeping Mr Zuma in power (Marais, 2018). This reality resulted in cadre deployment on all levels of government, and in the intelligence services (Hoffman, 2018; Van Den Berg, 2018:271). David Mahlobo was appointed as Minister of State security in 2014. He accompanied President Zuma on various state visits abroad, earning himself the title of “Zuma's Prime Minister” (Haffajee, 2017). The White Paper on Intelligence (1995) plays an important role in the approach to security and intelligence in South Africa, as it highlights among other things the purpose of intelligence (South Africa, 1995:2). The importance of this purpose was also highlighted by Minister of State Security, Dipuo Letsatsi-Duba, in her recent budget speech (2018:3). The Minister indicated that there is an urgent need to look into the SSA’s “failure of its governance and operational capacity” (Letsatsi-Duba, 2018:3). According to the Minister the problems arose from “systemic structural and governance weaknesses” because the agency has been in a “perpetual state of transition” (Letsatsi-Duba, 2018:3). The situation within the SSA has forced President Ramaphosa to appoint a high-level review panel in June 2018, headed by former Police Minister Sydney Mufamadi (Mahlase, 2018). According to a media statement by the Presidency, “the panel must seek to identify all material factors that allowed for some of the current challenges within the agency so that appropriate measures are instituted to prevent a recurrence”. The main objective of the review panel is to assist in ensuring a

responsible and accountable NI capability for the country in line with the Constitution and relevant legislation" (SSA, 2018).

Lack of legislative framework within the South African context

The SSA is faced with a lacking legislative framework for the interception of social media. Although various laws are relevant to social media and cyber issues, Swart (2018) is of the opinion that social media surveillance is currently unregulated in South Africa. The NCC at Musanda (Head Quarters of the SSA) has interception facilities that include bulk monitoring of telecommunications, conversations, e-mails, text messages and data. However, foreign SIGINT falls outside the spectrum of RICA (Swart, 2011). Currently there is no legislation governing the centre (Swart, 2011). Justice and Correctional Services Minister, Michael Masutha, indicates that the Department is in the process of introducing amendments to the RICA (70 of 2002) to close loopholes that allow for mass surveillance (Swart, 2017; Writer, 2018).



Source: Own construct

Figure 70: Findings of this study

A summary of this study's findings is depicted in Figure 70. The South African intelligence community has to safeguard national security. The main conclusion from these findings is

that there is a need for a new intelligence framework within the South African intelligence environment. This framework should include new sources of information such as SOCMINT.

These findings have raised various issues impacting on intelligence organisations and influencing their relevance within the new global security environment. Agrell (2012:122) is of the opinion that the current global environment has complicated the role of intelligence services and there are various challenges that are affecting the progress and function of intelligence. The study subsequently offers several recommendations.

8.6.2 Recommendations

In order to survive, any modern organisation should be dynamic and able to adapt to the changing global environment (Jackson & Jackson, 1997:3; Jackson, 2000:210). This is also the case with intelligence organisations; to survive they must adapt to the changing security environment.

Chapter 5 (see Section 5.2) explains that the main role and purpose of intelligence services is to preserve national security and to warn the government of threats against the country. This implies that intelligence is aimed at reducing uncertainty and managing potential risks that come with this uncertainty (Miller, 2008:337).

This study makes the following recommendations to ensure that the South African intelligence community remains relevant in the information age:

- New strategic intelligence framework: Intelligence reforms are imperative. However, reforms should be broader than the coordination issues. The reforms should include a new framework for intelligence that includes new sources such as SOCMINT to carry the intelligence community into the information age.
- New technical skills and expertise: The changed global environment requires new technical skills and expertise. The lack of specialisation can be addressed by using private companies to assist with the monitoring of social networking sites. The government can even go as far as buying a stake in that particular company (Eijkman & Weggemans, 2012:290).
- Leadership with intelligence background: The continuity of leadership is of great importance to motivate the workforce and to implement the new framework and all the changes.

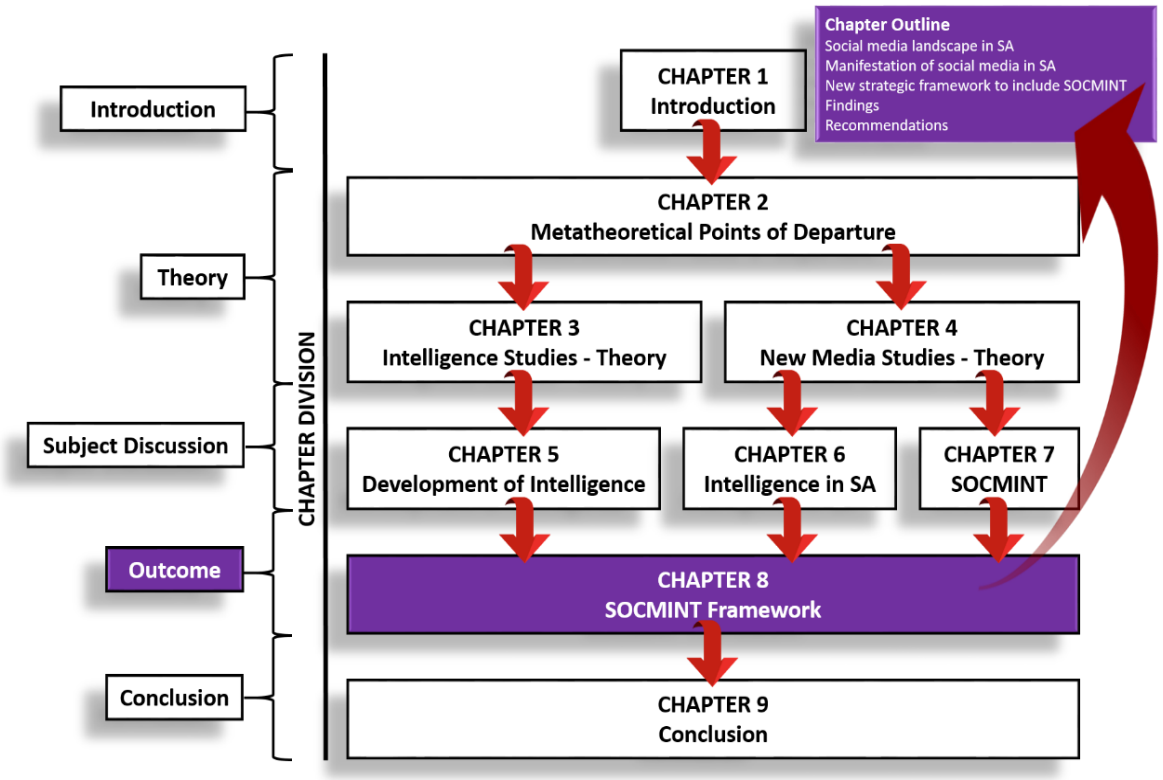
- New strategies: It is necessary to develop new recruiting, collection and analysis strategies that will fit the new threats such as terrorism, energy security and transnational organised crime (Alotaibi, 2010:28-46).
- Improve analytical skills: There is an urgent need to improve analytical skills and to train experts on new threats mentioned in the previous point (Alotaibi, 2010:44).
- Improved technology skills: There is a need for analysts and collectors that are well skilled in technology. In order to play a significant role in global issues, the policy maker has to embrace the new technology changes and implement information from the intelligence community (Teitelbaum, 2004:8).
- Agreements with private companies: The intelligence community cannot always keep up with the latest technology developments as a result of budgetary constraints (Berkowitz, 1997:111). However, they can take advantage of private sector innovation through cooperation agreements.
- Use of artificial intelligence: Intelligence organisations can use artificial intelligence to help sift through social media data.
- Legislative framework: A legislative framework to include the surveillance of social media (SOCMINT) should be designed.

8.7 Conclusion

The current South African security environment is being influenced by various issues that impact the intelligence situation. Most of challenges can be traced back to the continuous development of communication technologies. These technologies have created a virtual environment in which the intelligence communities should be able to operate. Furthermore, applications of the communication technologies have shaped new platforms for socialising and with it a new type of source, SOCMINT. The intelligence communities have to become accustomed to new communication technologies and its applications and advantages for the intelligence process to remain relevant. In contrast with Goodman's (2008:3) comments referred to in the introduction ("the world is less dangerous today than it was a decade ago"), Meyer (1987:93) is of the opinion that the role of intelligence will increase in future because the "world is not going to become a less complicated place". The world has not become a safer place; threats have increased and are more complex. Furthermore, the intelligence community is faced with technological developments that are changing on a continuous basis. These changes affect every aspect of the intelligence process and have implications for the traditional way in which intelligence has been conducted (Degaut, 2016:509). As indicated in the introduction of this chapter, intelligence services should change and adapt to

the new information environment, from there the new strategic framework proposed in this research.

In order to reach the goal of developing a strategic framework for the national security environment in South Africa, the social media in South Africa should be contextualised. One of the focus areas of this chapter was therefore to highlight social media and SOCMINT in the South African situation. The chapter began with a description of the social media landscape in South Africa. This section was followed by the discussion of the manifestation of social media use in the country. Three threats were identified within the South African context: protest movements, propaganda and criminal activities. In the next section a new strategic framework for the inclusion of SOCMINT in the intelligence environment was developed. This was followed by a discussion on findings and recommendations of this study. A summary of the chapter and how it relates to other chapters is presented in the figure below.



Source: Own construct

Figure 71: Chapter 8 Summary

This chapter meets the main objective of the study, namely *to investigate the threats and opportunities that social media presents, and based on a detailed research of the current*

intelligence theories, incorporate SOCMINT into a strategic framework for the security environment. The next chapter concludes this study.

CHAPTER 9: CONCLUSION

All agree that timely, accurate and usable intelligence will be critical to the successful conduct of war in the twenty-first century, perhaps more so than in any previous era.
Dupont (2003:15)

9.1 Introduction

The world is being bombarded by changes across the political, economic, security and social spectra. One of the main drivers behind these changes is information communication technology. These changes have major implications for the intelligence community in terms of both new threats and opportunities. These technologies have had a major impact on social interaction in the form of social media. Social media has gained popularity over the past ten years, mainly because of its broadcast speed and inexpensiveness.

As highlighted on several occasions, social media is one of the most significant outcomes of the internet and communication technology development. This new manifestation has motivated the study for the following reasons:

- New phenomenon: Social media is a new occurrence that affects all aspects of our daily activities, including political, economic and security developments.
- Implications for national security: As this is a new phenomenon, there is a lack of understanding of its security implications. The intelligence community has to fully understand this new phenomenon in relation to the threats against and opportunities for national security.
- A new source of information – SOCMINT: The intelligence community within South Africa does not fully understand the potential and threats of this new source and it has therefore not yet been included in intelligence strategies.

With this in mind, the focus of this chapter is addressed by means of five sections. In the first section, the discussion centres on the application of this study within the intelligence context. Secondly, this chapter evaluates the study against the objectives as set out in Chapter 1 to determine if the research objectives have been met. The next section deliberates the contributions of this study. This is followed by a discussion on future studies. The chapter concludes with a section that focuses on final recommendations.

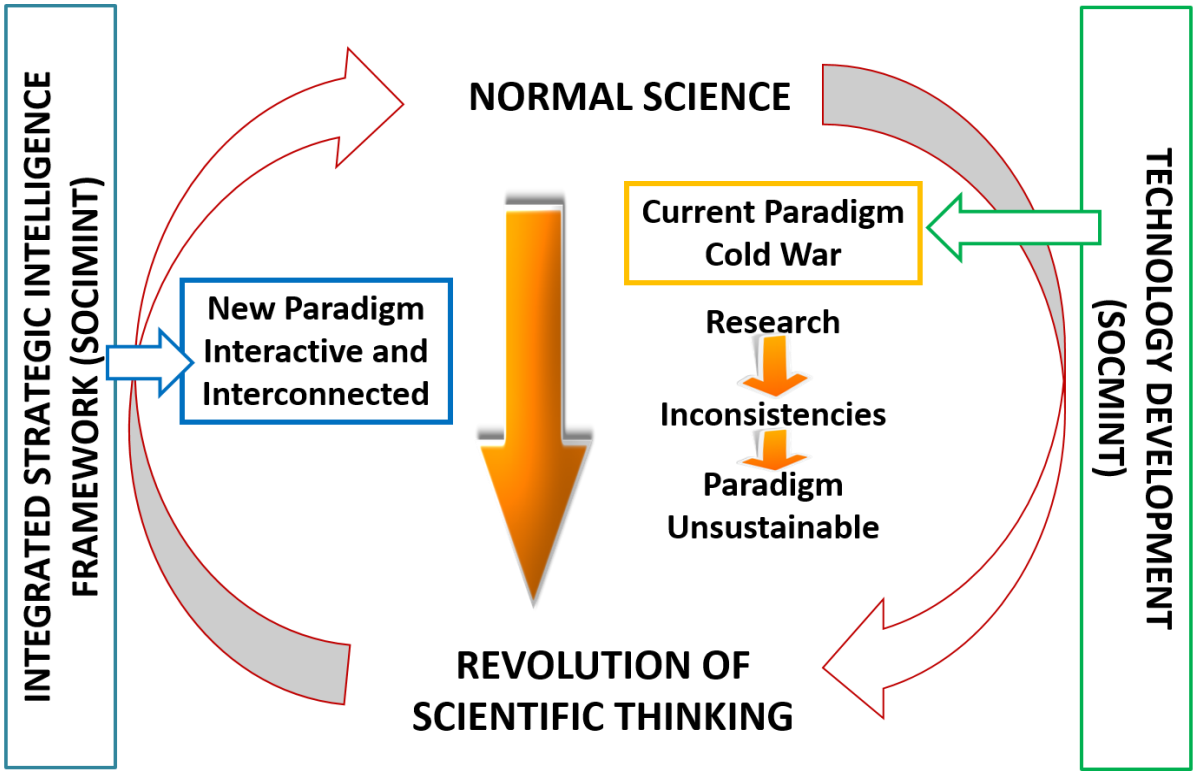
9.2 Application of this study

On conclusion of this study, it is pertinent to examine its applications within the South African intelligence environment. The primary aim of this study at hand was to develop a strategic framework for the national security environment in South Africa that includes SOCMINT as a source of information. In 1946 Albert Einstein said that “a new type of thinking is essential if mankind is to survive and move towards higher levels” (Chase, 2015). This quote remains relevant, especially at a time where technological change affects every aspect of our daily activities.

A new type of thinking has to develop within the intelligence environment. This study expressed on various occasions that the intelligence community within the South African context has not fully embraced new technology, especially SOCMINT. Furthermore, the study also indicated that intelligence is still stuck in the one dimensional Cold War paradigm where threats are mainly viewed as of a military nature with a limited number of information sources available for intelligence purposes (Lahneman, 2010:203). In order to remain an important role player within the security environment, the South African intelligence community should adopt a new paradigm. Chapter 2 (section 2.4.5) discussed the importance of a paradigm and explained how, according to Kuhn (1996:12), a paradigm can change and evolve and explained the need for a paradigm change within the intelligence environment (section 2.4.5). This paradigm change should be grounded in the implementation of the proposed strategic framework (discussed in Chapter 8).

The paradigm change is depicted in Figure 72 below. Kuhn (1996:12) explains that the history of a science is characterised by a period of “normal science” when research is done according to the recognised paradigm. However, as more research is conducted and inconsistencies are identified, the paradigm becomes unsustainable and this results in a “revolution” (Kuhn, 1996:12). This revolution causes a change in paradigm. This cycle can be applied to this study as well. Developments in technology, especially in relation to ICT, have increased the threat perspective to such an extent that security can no longer be linked to military threats only. ICT has created a borderless environment with threats such as transnational organised crime, human smuggling, human trafficking, drug trafficking and terrorism. This situation has challenged the Cold War paradigm, making it unsustainable. This study postulates that the ICT environment has created an environment where every entity on the globe can communicate directly with another using a variety of mediums. They do not have to take borders into account, and an action in one part of the world affects the globe in its entirety. In Chapter 2 the author coined this the “interactive and interconnected”

paradigm. This paradigm change necessitates a new integrated strategic intelligence framework where sources from the ICT background, such as SOCMINT, can be included.



Source: Own construct

Figure 72: New intelligence paradigm

With the application of this study clarified, the next section evaluates this study against the background of the objectives as formulated in Chapter 1.

9.3 Evaluation of this study

The objectives in **Chapter 1** were derived from the central theoretical statements. The research statement that underpinned this study was formulated as follows: *A systematic investigation of intelligence and social media is conducted to develop a strategic framework to incorporate the new phenomenon of SOCMINT into the intelligence environment, explaining its role within the intelligence cycle, its application as a source of information and the threats and opportunities related to it.* This research statement led to the following central theoretical statement: *Social media is a new source of intelligence that creates threats and provides opportunities for the intelligence community in South Africa. It is therefore important to develop a strategic framework that includes SOCMINT to mandate and guide the*

application of this source of intelligence within the intelligence environment. Various research objectives were identified to pursue this scientific investigation.

The first objective focused on constructing key metatheoretical points of departure relevant to this study. The study is a combination of intelligence studies and new media studies. In order to understand the new phenomenon of SOCMINT within the security context, it is important to first provide the theoretical foundation. This was done in **Chapter 2**, which focused on compiling a metatheoretical framework to guide and comprehend this study. A metatheoretical basis is of great importance as a guide to the researcher and for a better understanding of the scope of the study.

The metatheoretical framework for this particular topic was divided into two separate sections. The first part focused on the research philosophy applicable to this study. This discussion included the ontology, epistemology and methodology. For the purposes of this study, an anti-foundationalist ontology, an interpretivist epistemology and a qualitative methodology were followed. The second part of the metatheoretical framework concentrated on the components of social research. These components included pre-scientific consciousness, science and scientific knowledge, subject or discipline, paradigm, conceptual frameworks and concepts. Each component was explained in terms of social science research and applied to intelligence studies and new media studies. The chapter concluded with a metatheoretical framework that was applied throughout the study. This metatheoretical framework served the main aim of this study, namely constructing a strategic intelligence framework to include the SOCMINT phenomenon in the intelligence environment.

The next objective was to construct a metatheoretical, theoretical and conceptual orientation relevant to intelligence studies. This was the key emphasis of **Chapter 3.** The metatheoretical framework that was designed in Chapter 2 was applied to conceptualise intelligence studies as one pillar of this study. The outcomes of this chapter include the following:

- Discipline: Intelligence studies is classified as a social science with academic links to political science, international relations and security studies.
- Conceptual frameworks: Three conceptual frameworks were identified and discussed in relation to intelligence studies. The first framework is typology. The typology of the intelligence service in a country is closely linked to the political regime. In the case of South Africa, the political regime could be classified as a hybrid state and therefore the

intelligence service is less democratic, less accountable and more independent. The second framework is models. The best known model in intelligence studies is the intelligence cycle. Even though the idea of a cycle is widely debated, it remains the preferred model for most intelligence services. The final conceptual framework discussed was theories. The preferred theory for the purposes of this study is postmodernism. This theory provides an explanation of the current security environment where states are no longer the only role players in international politics.

- Concepts: The final section of this chapter addressed the concept of intelligence. There is currently no agreed term for intelligence. On this matter the following definition was constructed for this study: Intelligence involves the collection of information pertaining to all threats and opportunities from all available sources; the analyses, integration and interpretation of information into a product; and the timeous dissemination of the final product to the national client to assist in policy decisions.

The chapter concluded with a conceptual framework to understand the intelligence pillar of SOCMINT.

In order to complete the metatheoretical framework for this study, **Chapter 4** focused on the metatheory and theory of new media studies. The outcome of this chapter included:

- Discipline: New media studies belongs to communication science and, just like intelligence studies, is classified as a social science.
- Tradition: The tradition in relation to new media studies that is relevant to this study is phenomenology. The focus of this study is the social media phenomenon and how the information produced from this phenomenon (SOCMINT) can be used within the intelligence environment.
- Paradigm: Within the framework of new media studies, the digital media paradigm is applicable to this study. The elements of this paradigm include two-way communication in real time. Access is user-determined, content is user-driven and it is in a multi-media format. These elements all describe social media and it is therefore appropriate to apply the new digital paradigm.
- Conceptual frameworks: The three conceptual frameworks identified in Chapter 2 (typology, models and theories) were applied to new media studies. The typology of new media was discussed and old and new media were compared. The functional building block model was identified and applied to social media within the intelligence environment. This model assists the intelligence community to monitor, understand and

respond to social media activities. The final conceptual framework is theory. For the purposes of this study, three theories were identified. These include social network, uses and gratification and interactivity theories. While network theory can assist the intelligence community to understand networks within the social media phenomenon, uses and gratification theory explains the reasoning behind the uses of social media. The last theory of interactivity also applies to this study, as interactivity is associated with new communication methods and user generated content, such as social media.

- Concepts and definitions: The final segment discussed concepts such as hypertext and social media sites.

The chapter concluded with a conceptual framework to understand SOCMINT, including intelligence studies and new media studies.

The next objective was to study the global environment and to explain how technology development has influenced the evolution and progress of intelligence. Social media, and specifically SOCMINT, is one of the recent results of technology development. However, it is not the first time that technology influenced the progress of intelligence. The historic relationship between intelligence and the role of technology was explained in **Chapter 5.** The central goal of this chapter was to indicate how the development of technology played a crucial role in the evolution of the intelligence profession. In analysing the history of intelligence and technology, two timeframes are significant. The first is the period of the Great Wars (World War I and II) when SIGINT played a crucial role in the outcome of the wars. The second timeframe is the post-Cold War period. This era was characterised by digital communication, virtual reality and a change in social interaction. During both these timeframes technology played a crucial role in the development of intelligence and national security.

The fourth objective was to examine the progress of intelligence and the impact of technology within the South African context. This objective was addressed in **Chapter 6.** This chapter concluded with a table to illustrate the intelligence and technology developments in South Africa.

The next objective was to study social media to identify and understand the threats and opportunities associated with this phenomenon. In order to compile a strategic framework for the national security environment that takes SOCMINT into account, it is of great importance to understand the phenomenon of social media. In **Chapter 7,** social media and SOCMINT were explained in detail. This chapter provided a detailed history of the internet. This formed

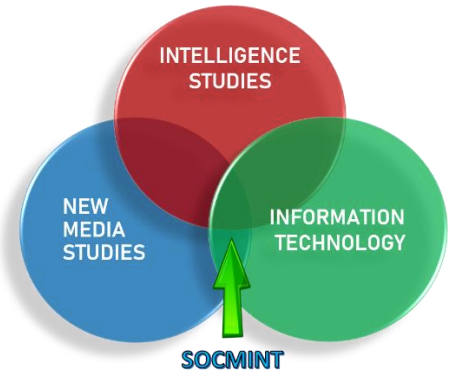
the basis for the next discussion, which focused on social media. This section defined social media, explained its origins, characteristics, functions and applications. The next section focused on the global digital landscape. In this section the growth of the internet and social media users is discussed to illustrate the extraordinary growth of this phenomenon. The threats and opportunities of social media were also cited. The final section of this chapter examined the application and challenges of SOCMINT.

The primary objective of this study was to investigate the threats and opportunities of social media and to compile a strategic framework to incorporate SOCMINT into the intelligence environment based on the research. This was the main focus of **Chapter 8**. The first section of the chapter focused on social media landscape within the South African context. In the following section, a new intelligence framework was developed to incorporate SOCMINT into the intelligence environment. This framework contains four levels. The first level is the scientific research framework that provides the theoretical foundation and departure points for the new framework. The second level is the operationalisation of the framework. This level includes five components that are of importance when operationalising this framework. The components are intelligence purpose, intelligence fields, intelligence elements, intelligence processes and intelligence priorities. The third level focuses on principles guiding intelligence and includes client relationship, efficiency and information sharing. The final level is governance, which includes legislation, transparency, accountability and oversight. The chapter concluded with findings and recommendations.

Closely linked to the evaluation presented above is the contribution of this study. This is discussed in great detail in the next section.

9.4 Contribution of this study

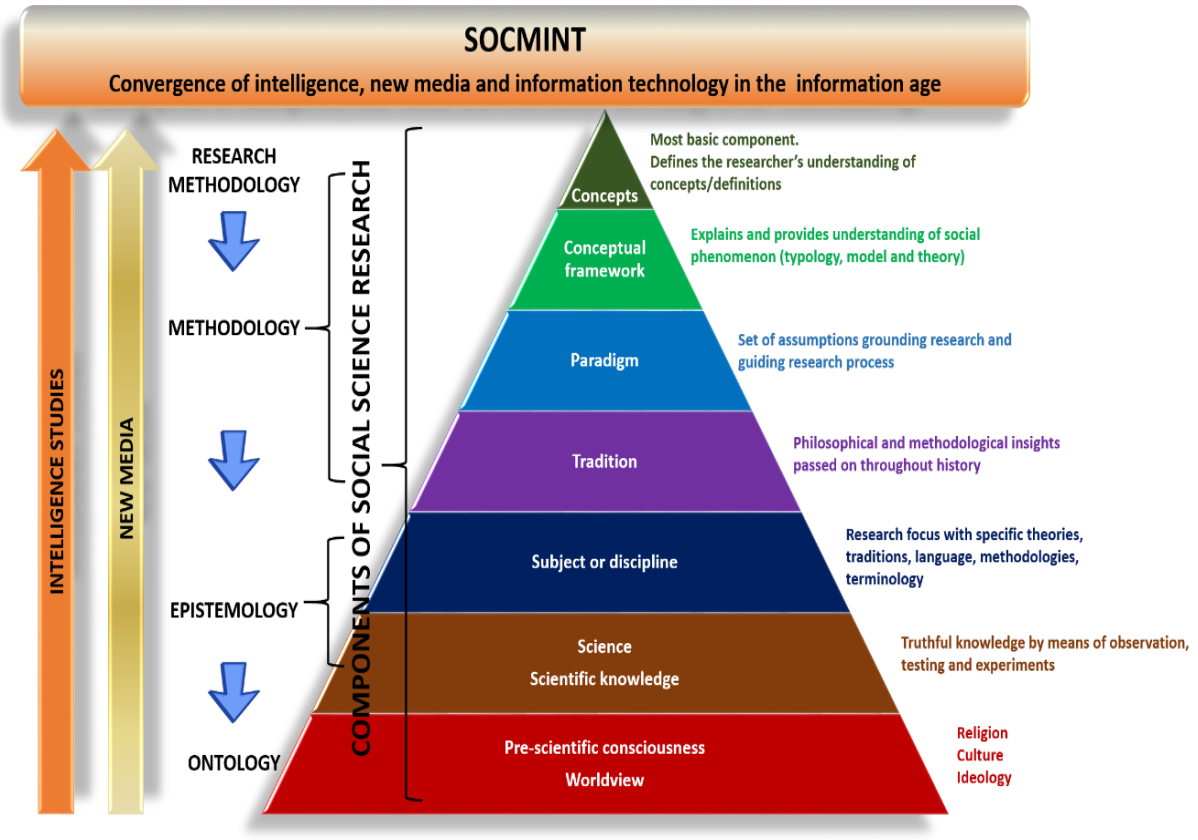
As explained in Chapter 2, the aim of any academic research is to contribute to scientific knowledge. The contribution of this study can be measured on two levels: the theoretical level and the operational level. It was important to first establish the academic focus of this study. The study is a convergence of three study fields: intelligence studies, new media studies and IT (Figure 73). However, the main pillars are intelligence studies and new media studies. IT is merely the enabler (platform) and was not included as part of the metatheoretical framework.



Source: Own construct

Figure 73: SOCMINT: Focus of this study

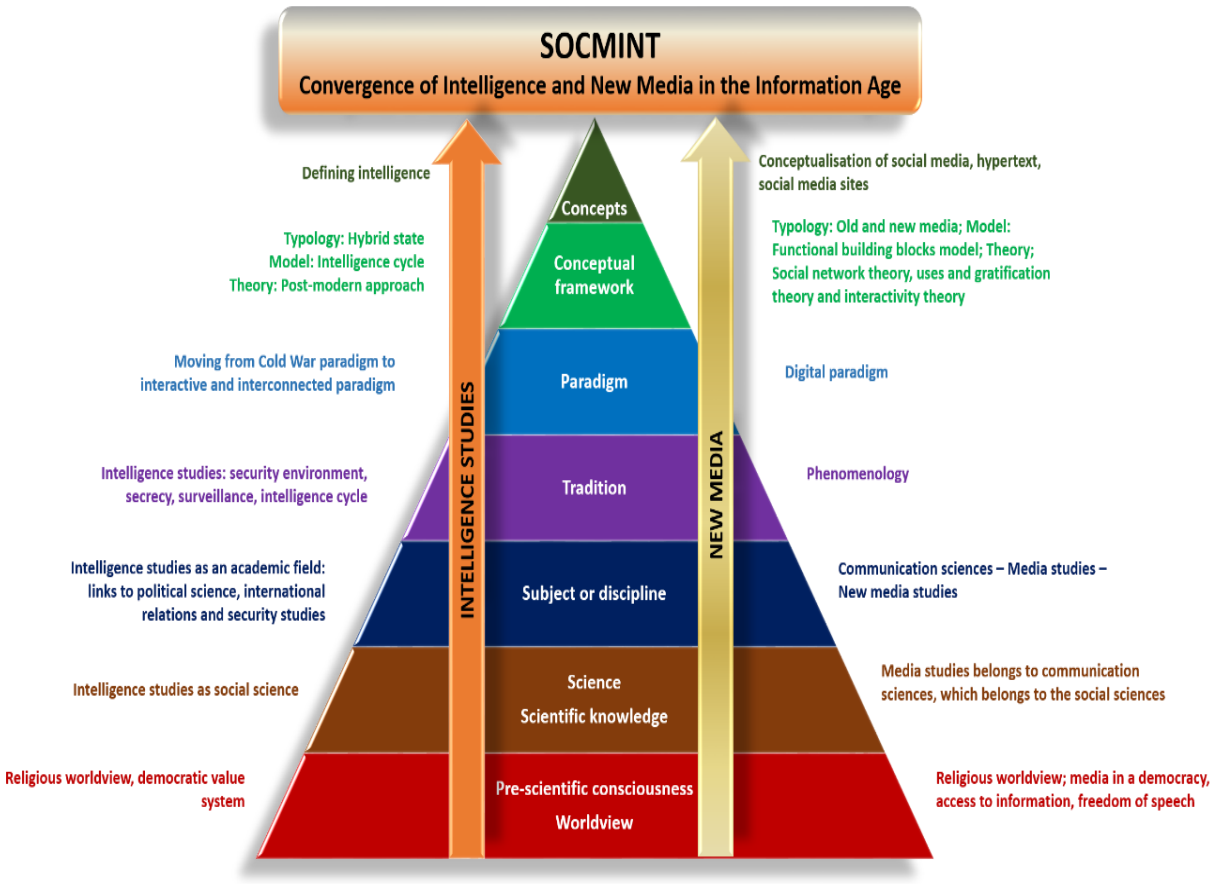
Once the academic focus had been established, a metatheoretical framework was developed to indicate the academic parameters of this study. The study identified seven components of social research that were used to compile the metatheoretical framework (Chapter 2). This framework is depicted in Figure 10 (repeated) below.



Source: Adapted from Duvenhage, 1994:60; Greffrath, 2015:29

Repeated Figure 10: Conceptual framework for understanding social science research in reference to SOCMINT

The metatheoretical framework was applied to intelligence studies and new media studies to compile a metatheoretical model to understand the phenomenon of SOCMINT. As a young discipline, intelligence studies lacks an in-depth theoretical base. By developing a metatheoretical model, this study contributes to the broadening of theory and growing the body of knowledge within the field of intelligence studies. These components were examined against intelligence studies and new media studies. The final combined framework is illustrated in repeated Figure 37 below.



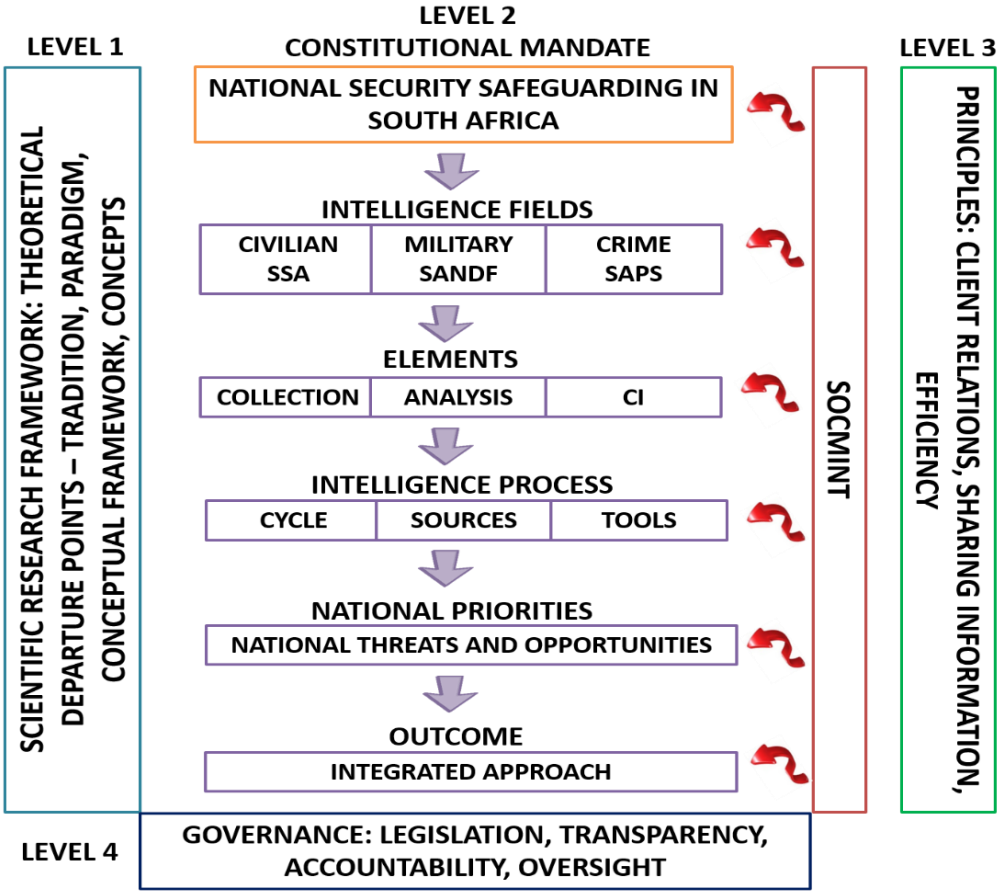
Source: Adapted from Duvenhage 1994:60; Greffrath, 2015:29

Repeated Figure 37: Meta-theoretical conceptual framework for understanding SOCMINT

This framework contributes to the theory base of intelligence studies and explains how SOCMINT can be understood.

The second contribution of this study is on the operational level. The study culminated in a strategic intelligence framework to include SOCMINT in the national security environment (Chapter 8). This new framework is divided into four levels (repeated Figure 67 below). The first level is the scientific research framework that deals with the theoretical departure points.

These include traditions, paradigms, conceptual frameworks and concepts related to intelligence. The next level is the operationalisation of the framework and it refers to the purpose of intelligence, fields of intelligence, elements of intelligence, the intelligence process and NIPs. The third level is principles that are crucial to this framework. These include client relationship, information sharing and efficiency. The final level is governance and includes issues such as legislation, accountability, transparency and oversight.



Source: Own construct

Repeated Figure 67: Conceptualised integrated strategic intelligence framework for SOCMINT

This study has managed to meet the objectives as set out in Chapter 1. Furthermore, the strategic framework (explained above) offers a response to the central theoretical statement. The section below highlights some opportunities for future studies.

9.5 Future studies

While this study developed a new strategic framework for the inclusion of SOCMINT in the intelligence environment, there are various issues that still need further examination and

research. One important aspect is the design of a new legislative framework to include social media surveillance. As mentioned previously, the South African legislation does not provide for social media surveillance. It is of great importance to start looking into how to best include social media within a legislative framework and still take freedom of speech and the Constitution into account. Another important contribution could be research into the development of new strategies with regard to recruiting of sources as well as personnel, collecting of information and analysing of data within the new intelligence environment of cyberspace. Intelligence strategies are still focused on the physical environment, and with the development of communication technologies, there is an urgent need to take cyberspace into consideration as well. With regard to the theoretical base of intelligence studies, further investigation is needed in relation to the postmodern approach to the field.

9.6 Recommendations

As discussed in Section 9.4, this study has contributed to the theoretical foundation of intelligence studies. Moreover, it has also developed a strategic framework for the inclusion of SOCMINT in the intelligence environment. This framework will assist the South African intelligence community to manage two distinct aspects that affect its activities. On the one hand there is a constant change in technological development that should be taken into consideration to remain relevant in the global arena of information overload. The second aspect is the global, regional and domestic landscape (security and political) that also influences the priorities of the intelligence community in South Africa. In this environment it is crucial to provide the client (government) with national strategic intelligence products that would enable them to make and implement policy decisions for ensuring national security. It is therefore imperative to implement a new strategic intelligence framework that is based on an integrated and holistic approach that contains a broad base of sources, including SOCMINT (Figure 74).

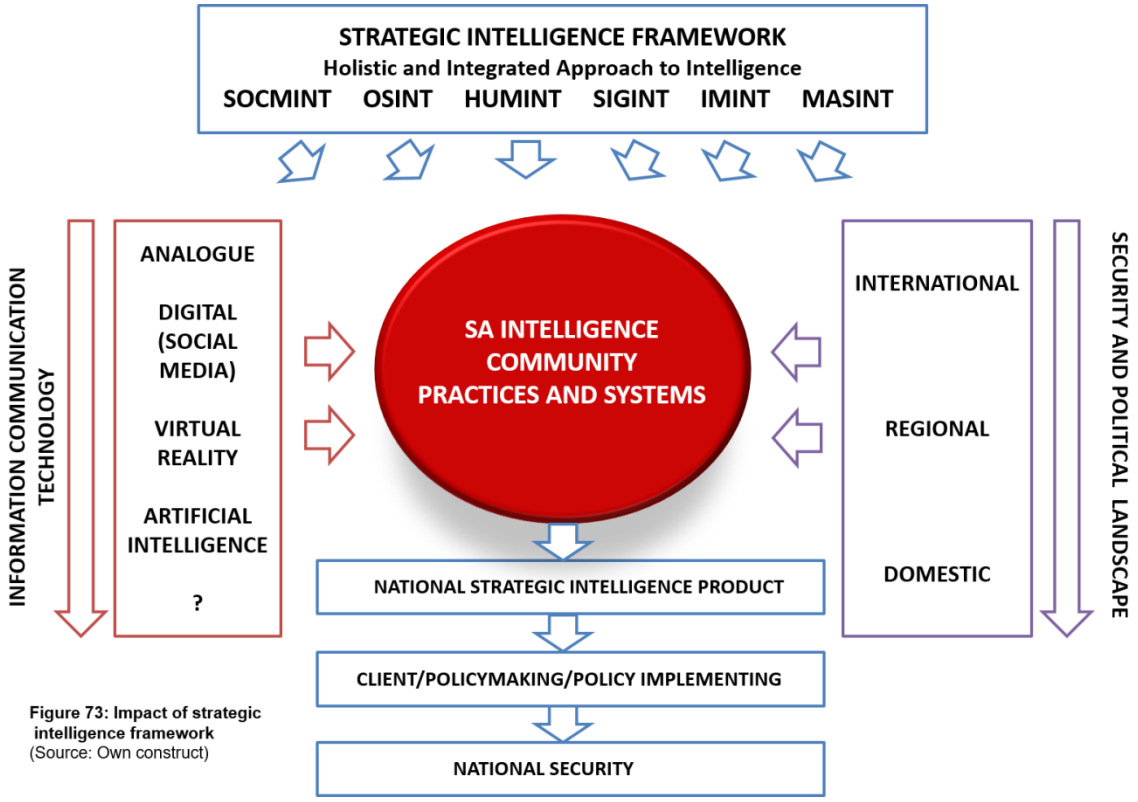


Figure 73: Impact of strategic intelligence framework
(Source: Own construct)

Source: Own construct

Figure 74: Impact of the strategic intelligence framework

It is recommended that the intelligence community in South Africa apply this framework to include SOCMINT in the intelligence context so that they can continue to play a crucial role in safeguarding national security.

9.7 Conclusion

The internet, and specifically social media, is increasingly being used as a communication method. However, this tool is also being used by terrorist organisations, political groups and crime syndicates to recruit members, to communicate, and to organise and plan events. It is these activities that create problems for national security, which is why this phenomenon should be studied and examined. This communication tool not only poses threats to national security, it also provides opportunities in the form of SOCMINT. This is an important tool that needs more attention within the intelligence community. In order to remain relevant and be the intelligence provider of choice, the intelligence community will have to include SOCMINT in the intelligence framework and stay ahead of, or at least on par with technological developments.

The future success or failure of intelligence organisations will not only depend on the effective management of challenges resulting from the new proposed paradigm, but will also be influenced by an intelligence organisation's ability to integrate and institutionalise SOCMINT. Along with the challenges of transformation, a future intelligence service in South Africa should identify, operationalise and institutionalise SOCMINT.

This is the challenge of the 21st century.

BIBLIOGRAPHY

Abbate, J. 1999. Inventing the internet. Boston, MA: The MIT Press.

Abdulhamid, S.M., Ahmed, S., Waziri, V.O. & Jibril, F.N. 2011. Privacy and national security issues in social networks: the challenges. *International Journal of the Computer, the Internet and Management,* 19(3):14–20.

Abrams, D. & Hogg, M. 2004. Metatheory: lessons from social identity research. *Personality and Social Psychology Review*, 8(2):98–106.

Achinstein, P. 2011. Scientific knowledge. (*In* Bernecker, S. & Pritchard, D., *eds*. The Routledge companion to epistemology. New York: Routledge. p. 346–357).

Aday, S., Farrel, H., Lynch, M., Sides, J., Kelly, J. & Zuckerman, E. 2010. Blogs and bullets: new media contentious politics. https://www.files.ethz.ch/isn/120788/pw65.pdf Date of access: 14 Aug. 2017.

Africa, S.E. 2006. Policy for managing access to intelligence information in post-apartheid South Africa. Johannesburg: University of the Witwatersrand. (Thesis – PhD).

Africa, S.E. 2009. South African intelligence services: a historic perspective. (*In* Africa, S.E. & Kwadjo, J., *eds*. Changing intelligence dynamics. Birmingham: GFN.SSR. p. 61–94).

Africa, S.E. 2012. The policy evolution of the South African civilian intelligence services: 1994 to 2009 and beyond. www.repository.up.ac.za/bitstream/handle/2263/africa_policy(2012).pdf Date of access: 10 Feb. 2014.

Agrell, W. 2012. The next 100 years? Reflections on the future of intelligence. *Intelligence and National Security,* 27(1):118–132.

Ahuja, C. 2015. Differences between traditional media and new media. https://www.vskills.in/certification/blog/differences-between-traditional-media-and-new-media/ Date of access: 23 June 2018.

Al-Menayes, J. 2015. Motivations for using social media: an exploratory factor analysis. *International Journal of Psychological Studies*, 7(1):43–50.

Alotaibi, Y.B. 2010. Revitalising the CIA: intelligence reform in the Post-Cold War world. http://trace.tennassee.edu/utk_chanhonoproj/1385 Date of access: 16 Sept. 2017.

Anchin, J. 2008. Pursuing a unifying paradigm for psychotherapy: tasks, dialectical considerations and biopsychosocial system metatheory. *Journal of Psychotherapy Integration*, 18(3):310–349.

Andrew, C. & Dilks, D. 1984. The missing dimension: Government and intelligence community in the twentieth century. London: McMillan Publishers.

Andrus, D. C. 2005. The Wiki and the Blog: towards a complex adaptive intelligence community. https://poseidon01.ssrn.com/delivery.php?id=036104118122116089064065024115066091118034032080036086072003117090126069118100017095039031120001116015022099022065107124001114001062026011109105007102064125099055077078096024114120089102002010127112000064002098114006099111110108094109096092013000&EXT=pdf Date of access: 16 Aug. 2017.

Ariel, Y. & Avidar, R. 2015. Information, interactivity and social media. *Atlantic Journal of Communication*, 23:19–30.

Aronson, J.D. & Cowhey, P.F. 2015. The information and communication revolution and international relations. http://annenberg.usc.edu/sites/default/files/2015/08/11/The_Information_and_Communication_Revolution_and_International_Relations_0.pdf Date of access: 26 Jan. 2017.

Audi, R. 2003. Epistemology: a contemporary introduction to the theory of knowledge. New York: Routledge.

Babbie, E. 2008. The basics of social research. Belmont: Thomson Wadsworth.

Baldwin, D.A. 1995. Security Studies and the end of the Cold War. *World Politics*, 48(Oct):5–26.

Baldwin, D.A. 1997. The concept of security. *Review of International Studies,* 23:5–26.

Barnard, N. 2015. Geheime revolusie: Memoires van ‘n spioenbaas. Kaapstad: Tafelberg.

Baron, I. 2014. The continuing failure of international relations and the challenges of disciplinary boundaries. *Millennium – Journal of International Studies,* 43(1):224–244.

Bartlett, J. & Miller, C. 2013. The state of the art: a literature review of social media intelligence capabilities for counter-terrorism. London: Demos.

Bauman, Z. 2006. Liquid modernity. Cambridge: Polity Press.

Bay, S. 2007. Intelligence theories: a literary overview. www.sebastian.bay.se/content/intelligence_theories-a_literary_overview.pdf Date of access: 6 Apr. 2015.

Bellany, I. 1981. Towards a theory of international security. *Political Studies*, 29(1):100–105.

Berg, B.L. 2001. Qualitative research methods for the social sciences. Allyn & Bacon: London.

Berkowitz, B.D. 1997. Information technology and intelligence reform. *Orbis,* Winter: 107–118.

Bhattacherjee, A. 2012. Social science research: principles, methods and practices. http://scholarcommons.usf.edu/oa_textbooks/3 Date of access: 15 Dec. 2014.

Blaikie, N. 1993. Approaches to social enquiry: advancing knowledge. Cambridge: Polity Press.

Blaikie, N. 2010. Designing social research. Cambridge: Polity Press.

Bock, P.G. & Berkowitz, M. 1966. The emerging field of national security. *World Politics*, 19(1):122–136.

Bogost, I. 2017. Obama was too good at social media. https://www.theatlantic.com/technology/archive/2017/01/did-america-need-a-social-media-president/512405/ Date of access: 11 May 2018.

Booth, K. 1991. Security and emancipation. *International Security*, 2:198–213.

Booth, K. 2007. Theory of world security. New York: Cambridge University Press.

Booth, K. 2013. Foreword. (*In* Shepard, L., *ed*. Critical approach to Security Studies. Abington: Routledge. p. xv–xvii).

Borgatti, S.P. & Halgin, D.S. 2011. On network theory. http://ssrn.com/abstract=2260993 Date of access: 29 Jun. 2018.

Bowcott, O. & Ball, J. 2014. Social media mass surveillance is permitted by law, says top UK official. https://www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr Date of access: 18 May 2018.

Boyd, D.M 2009. Social media is here to stay. Now what? http://www.danah.org/papers /talks/MSRTechFest2009.html Date of access: 25 Apr. 2018.

Boyd, D.M. & Ellison, N.B. 2008. Social network sites: definition, history and scholarship. *Journal of Computer-Mediated Communication*, 13:210–230.

Boyd, D.M, Golder, S. & Lotan, G. 2010. Tweet, tweet, retweet: conversational aspects of retweeting on twitter. www.danah.org/papers/tweettweetretweet.pdf Date of access: 13 Aug. 2017.

Bradshaw, S. & Howard, P.N. 2017. Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf Date of access: 11 May 2018.

Breakey, J. 2017. Taking to the tweets: South Africa's relationship with protests and Twitter. https://memeburn.com/2017/02/south-africa-protests-twitter/ Date of access: 11 May 2018.

Breakspear, A. 2013. A new definition of intelligence. *Intelligence and National Security*, 28(5):678–693.

Briggs, B. 2017. UK spy agencies share social media data with foreign governments, say critics. https://theferret.scot/uk-spy-agencies-share-social-media-data-foreign-governments-say-critics/ Date of access: 18 May 2018.

Bruneau, T.C. 2001. Controlling intelligence in new democracies. *International Journal of Intelligence and Counterintelligence*, 14(3):323–341.

Brunty, J.L, Helenek, K. & Miller, L.S., *eds*. 2013. Social media investigation for law enforcement. Waltham: Anderson.

Bruton, E. 2014. Communication technology. (*In* International Encyclopedia of the First World War). http://encyclopedia.1914-1918-online.net/pdf/1914-1918-Online-wireless_telegraphy-2014-10-08.pdf Date of access: 11 Jan. 2017.

Burds, J. 2011. The second oldest profession. North-eastern University: Recorded Books.

Burrell, G. 2005. Sociological paradigms and organisational analysis. Burlington: Ashgate.

Buzan, B. 1983. People states and fear: The national security problem in international relations. Brighton: Wheatsheaf Books.

Buzan, B. & Hansen, L. 2009. The evolution of international security studies. New York: Cambridge University Press.

Buzan, B. & Little, R. 2001. Why international relations has failed as an intellectual project and what to do about it. *Millennium –Journal of International Studies,* 30(1):19–39.

Cambridge Dictionary. 2018. Fake news. https://dictionary.cambridge.org/dictionary/english/fake-news Date of access: 11 May 2018.

Campbell, S.H. 2013. Intelligence in the post-Cold War period. *Intelligencer: Journal of US Intelligence Studies*, 19(3):45–65.

Caparini, M. 2007. Controlling and overseeing intelligence services in democratic states. (*In* Born, H. & Caparini, M., *eds.* Democratic control of intelligence services: Containing rogue elephants. Hampshire England: Ashgate Publishing. p. 3–24.)

Carafano, J. 2011. Mastering the art of Wiki: understanding social networking and national security. www.ndu.edu/press/lib/images/jfq-60/jfq60_73-78_carafano.pdf Date of access: 9 Nov. 2013.

Carr, E.H. 1946. The twenty years' crisis 1919–1939: an introduction to the study of international relations. London: Mac Millan & Co.

Castells, M. 2010a. The power of identity. West Sussex: Wiley-Blackwell.

Castells, M. 2010b. The rise of the network society. West Sussex: Blackwell Publishing.

Cavelty, M.D. & Mauer, V., *eds*. 2010. The Routledge handbook of security studies. Oxon: Routledge.

Central, C. 2017. 5 things you need to know about the latest Bell Pottinger developments. https://northcoastcourier.co.za/92850/5-things-need-know-latest-bell-pottinger-developments/ Date of access: 18 May 2018.

Chase, C. 2015. Paradigms are made for shifting. https://creativesystemsthinking.wordpress.com/2015/10/19/paradigms-are-made-for-shifting/ Date of access: 29 Oct. 2018.

Chun, W.H.K. 2008. Digital media, history of. (*In* Donsbach, W., *ed*. The international encyclopedia of communication. Malden: Blackwell. p. 1314–1319).

Church, F. 2011. Covert Action: Swampland of American foreign policy. (*In* Johnson, L. & Wirtz, J., *eds*. Intelligence and national security: the secret world of spies. New York: Oxford University Press. p. 233–237).

Clapper, J. 2016. Worldwide threat assessment of the US intelligence community. https://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf Date of access: 15 Aug. 2017.

Clarke, R.A. 2012. Cyber war: the next threat to national security and what to do about it. New York: Harper Collins.

Clark, R.M. 2013. Intelligence analysis: A target centric approach. Washington, DC: CQ Press.

Classen, J.S. 2005. The craft of intelligence analysis and assessment: a training manual for intelligence analysts. (Unpublished).

Cleary, T. 1988. Sun Tzu: The art of war. Boston, MA: Shambhala Publications.

Clift, A.D. 2008. Intelligence in the internet era. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article06.html Date of access: 25 Jan. 2017.

Cohn, M. 2011. Social media vs. social networking. www.compukol.com/social%20Media%20vs%20Social%20Networking.pdf Date of access: 27 Apr. 2018.

Collins, A., *ed*. 2013. Contemporary security studies. New York: Oxford University Press.

Collins, K. 2015. Government pays companies to monitor you on social media. http://www.wired.co.uk/article/government-pays-companies-to-monitor-social-media-use Date of access: 18 May 2018.

Concise Oxford English Dictionary. 2004. New York: Oxford University Press.

Constitution ***see*** South Africa.

Cooper, R. 2002. The postmodern state. http://www.world-governance.org/article86.html Date of access: 2 Dec. 2016.

Corbetta, P. 2003. Social research: theory, methods and techniques. London: Sage Publications.

Cornish, J.J. 2017. Fake news reports hit Kenya's election build up. *Eyewitness News*, 31 July. Ewn.co.za/2017/07/31/fake-news-reports-hit-kenya-s-selection-build-up Date of access: 24 Aug. 2017.

Cox, M. 2012. Introduction to international relations. London: University of London.

Coyne, J., Neal, N. & Bell, P. 2014. Reframing intelligence: Challenging the Cold War doctrine in the information age. *International Journal of Business and Commerce*, 3(5):53–68.

Craig, R.T. 1999. Communication theory as a field. *Communication Theory*, 9(2):119–161.

Craig, R.T. 2009. Traditions of communication theory. (*In* Littlejohn, S.W. & Foss, K.A., *eds*. Encyclopedia of communication theory. Thousand Oaks: Sage. p. 958–963).

Cross, C. 2017. Why are African governments so worried by social media? Quartz Africa. https://qz.com/926162/african-governments-are-scared-of-social-media-from-cameroon-and-drc-to-gabon-and-gambia/ Date of access: 17 Oct. 2017.

Cybercrime and Cybersecurity Bill **see** South Africa.

Daigle, L. 2015. On the nature of the internet. www.cigionline.org/sites/default/files/gcig_paper_no7.pdf Date of access: 18 Apr. 2018.

Davis, G. 2018. Bill to regulate online content approved. http://ewn.co.za/2018/03/06/bill-to-regulate-distribution-of-online-content-approved Date of access: 29 May 2018.

DCAF (Democratic Control of Armed Forces). 2003. Intelligence practice and democratic oversight – A practitioners view. Occasional paper no 3. https://www.dcaf.ch/sites/default/files/publications/documents/op03_intelligence-practice.pdf Date of access: 12 March 2016.

DCAF (Democratic Control of Armed Forces). 2006. Intelligence services – Backgrounder. www.dcaf.ch Date of access: 21 Apr. 2017.

De Vaus, D. 2001. Research design in social research. London: Sage Publications.

De Vos, A., Strydom, H., Fouche, C. & Delport, C. 2011. Research at grassroots. Van Schaik: Pretoria.

Debruyne, E. 2015. Espionage. www.ecyclopedia.1914-1915-online.net/article/espionage Date of access: 14 Apr. 2016.

Defence Act **see** South Africa.

Degaut, M. 2016. Spies and policymakers: intelligence in the information age. *Intelligence and National Security*, 31(4):509–531.

Deleuze, G. & Guattari, F. 1994. What is philosophy? New York: Colombia University Press.

Department of Justice **see** South Africa. Department of Justice.

Difesa, M. 2012. Impact of social media on national security. http://www.difesa.it/SMD_CASD/IM/social_media_20120313_0856.pdf Date of access: 7 Feb. 2014.

Dix, H. 2011. Republic of Moldova at the end of an election marathon? www.kas.de/wf/doc/kas_21875-544-2-30.pdf?110209122237 Date of access: 9 May 2018.

Dlomo, D.T. 2004. An analysis of parliamentary oversight in South Africa with specific reference to the joint standing committee on intelligence. Pretoria: UP. (Dissertation - Masters).

Dolley, C. 2017. Social media in SA could be regulated, says Mahlobo. *News24*, 5 March. www.news24.com/southafrica/news/social -media-in-sa-could-be-regulated-says-mahlobo-20170305 Date of access: 16 Aug. 2017.

Donato, D. 2010. An introduction to the world wide web. (*In* Caldarelli, G., *ed*. Complex networks. Abu Dhabi: EOLSS Publishers. p. 59–67). https://www.eolss.net/Sample-Chapters/C15/E6-200-03.pdf Date of access: 11 May 2018.

Donnison, J. 2010. Israel 'using Facebook to recruit Gaza collaborators'. http://news.bbc.co.uk/2/hi/middle_east/8585775.stm Date of access: 18 May 2018.

Doorey, T.J. 2007. Intelligence secrecy and transparency: finding the proper balance from the war of independence to the war on terror. *Strategic Insights*, 6(3):1–13.

Dozier, D.M., Grunig, L.A. & Grunig, J.E. 1995. Manager's guide to excellence in public relations and communication management. Mahwah: Lawrence Erlbaum Associates.

Dubberly, H. & Pangaro, P. 2010. Introduction to cybernetics and the design of systems. http://pangaro.com/CUSO2014/Cybernetics_Book_of_Models-v4.6b-complete.pdf Date of access: 16 Jun. 2018.

Dugdale, J., Van De Walle, B. & Koeppinghoff, C. 2012. Social media and SMS in the Haiti earthquake. http://magma.imag.fr/sites/default/files/users/Julie%20Dugdale/final_dugdale_swdm.pdf Date of access: 11 May 2018.

Dulles, A.W. 1965. The craft of intelligence. New York: Signet Books.

Dupont, A. 2003. Intelligence for the twenty-first century. *Intelligence and National Security*, 18(4):15–39.

Duvenhage, A. 1994. Die transformasie van politieke instellings in oorgangstye: 'n Rekonstruksie, interpretasie en evaluasie van S.P. Huntington se teoretiese bydrae. Bloemfontein: Universiteit van die Oranje Vrystaat (UOVS). (Unpublished Thesis - DPhil.)

Easton, D. 1991. Political science in the United States: Past and present. (*In* Easton, D., Gunnell, J.G. & Graziano, L., *eds*. The development of political science: a comparative survey. London: Routledge. p. 275–290).

Eaton, T. 2013. Internet activism and the Egyptian uprisings: transforming online dissent into the offline world. (*In* Taki, M. & Coretti, L., *eds*. *Westminster papers in Communication and Culture*, 9(2):5–24).

Eijkman, Q. & Weggemans, D. 2012. Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? *Security and Human Rights*, 4:286–296.

Electronic Communication Security (Pty) Ltd Act **see** South Africa.

Etheridge, J. 2016. Permanent removal of UCT Rhodes statue gets green light. https://www.news24.com/SouthAfrica/News/permanent-removal-of-uct-rhodes-statue-gets-green-light-20161031 Date of access: 16 May 2018.

Farzindar, A. & Inkpen, D. 2015. Natural language processing for social media. San Rafael: Morgan & Claypool.

Fedorowich, K. 2005. German espionage and British counter intelligence in South Africa and Mozambique, 1939–1944. *The Historical Journal,* 48(1):209–230.

Ferris, J. 1988. The British army and signals intelligence in the field during the first World War. *Intelligence and National Security*, 3(4):23–48.

Fielding, N. & Cobain, I. 2011. Revealed: US spy operation that manipulates social media. https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks Date of access: 18 May 2018.

Finan, E. 2010. The immorality of covert action. *International Affairs Review*, 25 October. http://www.iar-gwu.org/node/214 Date of access: 14 Jun. 2017.

Fitsanakis, J. & Bolden, M. 2012. Social media as a paradigm shift in tactical intelligence collection. (*In* Nimokos, J.M., Ducci, S. & Bertacin, E., *eds*. MCIS Yearbook 2012. p. 28–40). http://rieas.gr/images/mcis2012.pdf Date of access: 18 May 2018.

Fordred, L.L. 1997. Wireless in the second Anglo Boer War 1899–1902. *The Transactions of the SA Institute of Electrical Engineers,* Sept(1997):61–71.

Fraustino, J.D., Liu, B. & Jin, Y. 2012. Social media use during disaster. https://www.start.umd.edu/sites/default/files/files/publications/START_SocialMediaUseduring Disasters_LitReview.pdf Date of access: 8 Aug. 2017.

Frieden, J. & Lake, D. 2005. International relations as a social science: rigor and relevance. https://scholar.harvard.edu/files/jfrieden/files/annalsapss-2005.pdf Date of access: 15 Dec. 2014.

Froget, J.R.L., Baghestan, A.G. & Asfaranjan, Y.S. 2013. A uses and gratification perspective on social media usage and online marketing. *Middle-East Journal of Scientific Research*, 15(1):134–145.

Garrett, R.K. & Edwards, P.N. 2007. Revolutionary secrets: Technology's role in the South African anti-apartheid movement. www.sahistory.org.za/sites.default/files/garrettedwards-revolutionarysecrets-prepress.pdf Date of access: 21 Jul. 2017.

Geldenhuys, D. 1984. The diplomacy of isolation: South African foreign policy making. Johannesburg: Macmillan South Africa.

General Intelligence Laws Amendment Act **see** South Africa.

Gill, P. 2006. What is intelligence theory. (*In* Treverton, G.F., Jones, G., Boraz, S. & Lipscy, P. Towards a theory of intelligence. Rand Corporation Workshop Report. p. 4–5). http://www.rand.org/pubi/larf/proceedings/2006Rand-cf219 Date of access: 2 Mar. 2015.

Gill, P. & Phythian, M. 2006. Intelligence in an insecure world. Cambridge: Polity Press.

Gill, P. & Phythian, M. 2012. Intelligence studies: some thoughts on the state of the art. *Annals of the University of Bucharest/Political Science Series,* 14(1):5–17.

Gill, P., Marrin, S. & Phythian, M., *eds*. 2009. Intelligence theory: Key questions and debates. New York: Routledge.

Glaser, C.L. 2013. Realism. (*In* Collins, A., *ed*. Contemporary security studies. New York: Oxford University Press. p. 14–27).

Goodman, A.E. 2008. Shifting paradigms and shifting gears: A perspective on why there is no post-cold war intelligence agenda. *Intelligence and National Security*, 10(4):3–9.

Goodman, A.E. & Berkowitz, B.D. 2008. Intelligence without the Cold War. *Intelligence and National Security Journal*, 9(2):301–319.

Gorry, F. 2001. Packet switching. www.erg.abdn.ac.uk/users/gorry/course/intro-pages.html Date of access: 11 Apr. 2018.

Greffrath, W.N. 2015. State dysfunction: the concept and its application to South Africa. Potchefstroom: North-West University. (Unpublished – PhD Thesis).

Gressang, D.S. 2007. The shortest distance between two points lies in rethinking the question: Intelligence and the information age technology challenge. (*In* Johnson, L.K. *ed*., Strategic intelligence the intelligence cycle. Westport, CT.: Praeger Security International. p. 123–142).

Griffiths, M. & O'Callaghan, T. 2002. International relations: The key concepts. London: Routledge.

Gross, G. 2018. Countries consider penalties for spreading 'fake news'. https://www.internetsociety.org/blog/2018/04/countries-consider-penalties-spreading-fake-news/ Date of access: 18 May 2018.

Grunig, J.E. & Hunt, T. 1984. Managing public relations. New York: Holt, Reinhart and Winston.

Gupta, R. 2013. Using social media for global security. Indianapolis: John Wiley & Sons.

Haffajee, F. 2017. David Mahlobo -- Zuma's 'Prime Minister'. https://www.huffingtonpost.co.za/2017/09/25/david-mahlobo-zumas-own-prime-minister_a_23221573/ Date of access: 14 Aug. 2018.

Halgin, D.S. 2012. An introduction to social network theory. http://jesuitnetworking.org/wp-content/uploads/2013/10/halgin_social_network_theory.pdf Date of access: 14 Aug. 2018.

Harris, J.D. 1998. Wire at war: Signals communication in the South African War 1988–1902. *Military History Journal*, 11(1). www.samilitaryhistory.org/vol111jh.html Date of access: 7 Jul. 2017.

Harrysson, M., Métayer, E. & Sarrazin, H. 2012. How 'social intelligence' can guide decisions. https://www.mckinsey.com/industries/high-tech/our-insights/how-social-intelligence-can-guide-decisions Date of access: 18 May 2018.

Hay, C. 2002. Political analysis: a critical introduction. Hampshire: Palgrave.

Hay, C. 2006. Political ontology. (*In* Goodin, R. & Tilly, C., *eds*. The Oxford handbook of contextual political analysis. Oxford: Oxford University Press. p. 78–96.)

Haynes, J., Hough, P., Malik, S. & Pettiford, L. 2017. World Politics: international relations and globalisation in the 21st century. London: Sage.

Hecht, G. & Edwards, P.N. 2010. The techno politics of the Cold War. (*In* Adas, M., *ed*. Essays on twentieth century history. Philadelphia: Temple University Press. p. 271–314).

Henderson, R.D. 1995. South African intelligence under De Klerk. *International Journal of Intelligence and Counter Intelligence,* 8(1):51–89.

Henn, M., Weinstein, M. & Foard, N. 2006. A short introduction to social research. London: Sage Publications.

Herman, M. 1996. Intelligence: power in peace and war. Cambridge: Cambridge University.

Heywood, A. 2002. Politics. Hampshire: Palgrave Macmillan.

Hill, R. 2013. Key characteristics that distinguish the Internet. www.apig.ch/Internet%203-characteristics.doc Date of access: 11 Apr. 2018.

HMICFRS (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services). 2011. The rules of engagement: A review of the August 2011 disorders. www.justiceinspectorates.gov.uk/hmicfrs/media/a-review-of-the-august-2011-disorders-20111220.pdf Date of access: 15 Aug. 2017.

Hobbes, R. 2018. Hobbes' internet timeline 25. www.zakon.org/robert/internet/timeline Date of access: 11 Apr. 2018.

Hodes, R. 2015. The Rhodes statue must fall: UCT's radical rebirth. https://www.dailymaverick.co.za/article/2015-03-13-the-rhodes-statue-must-fall-ucts-radical-rebirth/#.WvsXYaSFOM8 Date of access: 16 May 2018.

Hoffman, P. 2018. Cadre deployment: the underlying cause of state capture. https://www.dailymaverick.co.za/opinionista/2018-05-14-cadre-deployment-the-underlying-cause-of-state-capture/ Date of access: 14 Aug. 2018.

Hollis, M. & Smith, S. 1990. Explaining and understanding international relations. New York: Oxford University Press.

Holmes, D. 2009. New media theory. (*In* Littlejohn, S.W. & Foss, K.A., *eds*. Encyclopedia of communication theory. Thousand Oaks: Sage. p. 684–688).

Howard, P.N., Duffy, A., Freelon, D., Hussain, M., Mari, W. & Mozaid, M. 2011. Opening closed regimes: what was the role of social media during the Arab Spring. http://dx.doi.org/10.2139/ssrn.2595096 Date of access: 17 Aug. 2017.

Hulnick, A.S. 2006. What's wrong with the intelligence cycle? *Intelligence and National Security*, 21(6):959–979.

Hutton, L. 2007. Looking beneath the cloak: an analysis of intelligence governance in South Africa. Pretoria: Institute for Security Studies (ISS). (Paper no. 154, Nov 2007).

Intel Corporation. 2015. Internet surfing. https://www.intel.com/content/dam/www/program/education/us/en/documents/intel-easy-steps/easy-steps-activity-surf-internet.pdf Date of access 30 Apr. 2018.

Intelligence Services Act **see** South Africa.

Intelligence Services Amendment Bill **see** South Africa.

Intelligence Services Oversight Act **see** South Africa.

Internet Hall of Fame. 2016. Internet history. www.internethalloffame.org/internet-history/timeline Date of access: 16 Apr. 2018.

Internet Society. 2013. Internet society testifies before U.S. House of representatives on internet policy and internet freedom. https://www.internetsociety.org/news/press-releases/2013/internet-society-testifies-before-u-s-house-of-representatives-on-internet-policy-and-internet-freedom/ Date of access: 22 Apr. 2018.

Internet Society. 2016. Internet invariants: What really matters. An internet society public policy briefing. https://cdn.prod.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-InternetInvariants-20160926-nb.pdf Date of access: 18 Apr. 2018.

Irondelle, B. 2013. The new parameters of international security: Conceptual introduction. *Transworld*, April:4–5.

Ismail, N. 2017. Big Brother: Government surveillance efforts aimed at citizens social media data? http://www.information-age.com/government-surveillance-efforts-aimed-citizens-social-media-data-123469217/ Date of access: 18 May 2018.

Jabareen, Y. 2009. Building a conceptual framework: philosophy, definition and procedure. *International Journal of Qualitative Methods,* 8(4):49–62.

Jackson, D. 2000. Becoming dynamic: Creating and sustaining dynamic organisations. London: Palgrave Macmillan.

Jackson, J. & Jackson, D. 1997. A comparative introduction to political science. New Jersey: Prentice Hall.

Jackson, J. & Jackson, D. 2003. An introduction to political science: comparative and world politics. Ontario: Prentice Hall.

Jackson, R. & Sørensen, G. 2010. Introduction to IR: theories and approaches. 5th ed. Oxford: Oxford University Press.

Jenkin, T. 1995. Talking to Vula: the secret underground communication network of operation Vula. www.anc.org.za/content/talking-vula Date of access: 21 Jul. 2017.

Jensen, C.J., McElreth, D.H. & Graves, M. 2013. Introduction to intelligence studies. Baco Raton: CRC Press.

Jensen, J.F. 1998. Interactivity: tracking a new concept in media and communication studies. *Nordicom Review*, 19:185–204.

Johnson, J.B., Reynolds, H.J. & Mycoff, J.D. 2008. Political science research methods. Washington: CQ Press.

Johnson, L.K. 2007. Strategic intelligence: understanding the hidden side of government. Westport, CT: Praeger Security International.

Johnson, L.K. 2009. Sketches for a theory of strategic intelligence. (*In* Gill, P., Marrin, S. & Phythian, M., *eds*. Intelligence theory: key questions and debates. New York: Routledge. p. 33–53).

Johnson, L.K. & Wirtz, J. 2015. Intelligence and national security: the secret world of spies. New York: Oxford University Press.

Johnson, R. 1999. Post-Cold war security: the lost opportunities. www.isnethz.ch/digital-library/publications/detail/?ots591 Date of access: 18 Feb. 2014.

Jones, R. 1999. Security strategy and critical theory. Boulder: Lyn Rienner Publishers.

Kadushin, C. 2012. Understanding social networks: theories, concepts and findings. New York: Oxford Press.

Kahn, D. 2001. An historical theory of intelligence. *Intelligence and National Security Journal*, 16(3):79–92.

Kahn, D. 2006. The rise of intelligence. *Foreign Affairs*, 85(5):125–134.

Kallas, P. 2018. World map of social networks. https://www.dreamgrow.com/world-map-of-social-networks/ Date of access: 3 May 2018.

Kamffer, H.J.G. 1999. Om een scherpe oog in't zeil te houden: Die Geheime Diens in die Zuid Afrikaanse Republiek. Vanderbijlpark: North-West University. (Thesis – PhD).

Katz, E., Blumler, J.G. & Gurevitch, M. 1974. Uses and gratifications research. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.886.3710&rep=rep1&type=pdf Date of access: 18 Jun. 2018.

Kaufmann, F. 1958. Methodology of the social sciences. New York: The Humanities Press.

Kaul, V. 2012. Changing paradigm of media landscape in the digital age. *Journal of Mass Communication and Journalism*, 2(2):1–9.

Keefer, A. & Baiget, T. 2001. How it all began: a brief history of the Internet. *Vine*, 31(3):90–95.

Kemp, S. 2018. Digital in 2018: World's internet users pass 4 billion mark. https://wearesocial.com/blog/2018/global-digital-report-2018 Date of access: 12 Apr. 2018.

Kent, G. 1974. Espionage. London: Redwood Burn Limited.

Kent, S. 1966. Strategic intelligence for American world policy. Princeton: Princeton University Press.

Keohane, O. & Nye, J.S. 1998. Power and interdependence in the information age. *Foreign Affairs*, 77(5):81–94.

Kietzmann, J.H., Hermkens, I.P., McCarthy, B.S. & Silvestre, B.S. 2011. Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons,* 241–251.

Kiousis, S. 2002. Interactivity: a concept explication. *New Media and Society,* 4(3):355–383.

Klein, P. 2005. Epistemology. (*In* Craig, E., *ed*. The shorter Routledge encyclopaedia in philosophy. Oxon: Routledge. p. 224–227.)

Kohlmann, E.F. 2006. The real online terrorist threat. *Foreign Affairs,* 85(5):115–124.

Krahmann, E. 2005. From state to non-state actors: The emergence of security governance. (*In* Krahmann, E., *ed*. New threats and new actors in international security. New York: Palgrave Macmillan. p. 3–19).

Krause, K. & Williams, M.C. 1996. Broadening the agenda of security: politics and methods. *Mershon International Studies Review*, 40(2):229–254.

Krippendorf, K. 2008. Cybernetics. (*In* Donsbach, W., *ed*. The international encyclopedia of communication. Malden: Blackwell. p. 1152–1159).

Krishnan, A. 2009. What are academic disciplines? eprints.ncrm.ac.uk/783. Date of access: 28 Dec. 2014.

Kruys, G.P.H. 2006. Intelligence failures: causes and contemporary case studies. http://repository.up.ac.za/bitstream/handle/2263/3078/Kruys_Intelligence(2006).pdf?sequence=1 Date of access: 30 Mar. 2017.

Kubovich, Y. 2016. The Facebook squad: How Israel police tracks activists on social media. https://www.haaretz.com/israel-news/.premium-how-israel-police-tracks-activists-on-social-media-1.5400741 Date of access:18 May 2018.

Kuhn, S. 1996. The structure of scientific revolution. Chicago: University of Chicago Press.

Kuitenbrouwer, V. 2012. War of words: Dutch pro-Boer propaganda and the South African War (1899–1902). Amsterdam: Amsterdam University Press.

Lahneman, W.J. 2010. The need for a new intelligence paradigm. *International Journal of Intelligence and Counterintelligence*, 23(2):201–225.

Lang, M. 2017. Social media monitoring continues to concern civil rights groups. http://www.govtech.com/public-safety/Social-Media-Monitoring-Continues-to-Concern-Civil-Rights-Groups.html Date of access: 18 May 2018.

Lawless, F. 2012. America blindsided: The US Intelligence failures that led to 9/11. https://c.ymcdn.com/sites/www.iafie.org/resource/resmgr/2012_conference/faith_lawless_the_us_intell.docx Date of access: 30 Mar. 2017.

Lawlor, R. 2007. The age of globalization: Impact of technology on global business strategies. www.digitalcommens.bryant.edu>Honor>Honors>_cis>1 Date of access: 18 Feb. 2014.

Ledoux, S. 2002. Defining natural sciences. *Behaviorology Today*, 5(1):34–36.

Leedy, P.D. & Ormrod, J.E. 2014. Practical research: Planning and design. London: Pearson.

Leiner, B.M., Cerf, G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolff, S. 2009. A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, 39(5):22–28.

Leiter, M. 2014. Why people use social media. https://www.socialmediatoday.com.content/why-do-people-use-socail-media Date of access: 27 Apr. 2018.

Lerner, A.W. 2004. Espionage and intelligence, early historical foundations. (*In* Lerner, K.L. & Lerner, B.W., *eds*. Encyclopedia of espionage. Detroit: Gale group. p. 415–420).

Letsatsi-Duba, D. 2018. Budget vote speech of the Department of State Security by Hon. D. Letsatsi-Duba M.P., Minister of State Security. http://www.ssa.gov.za/Portals/0/SSA%20docs/Speeches/2018/MIN_Budget%20Vote%20Speech%2018%20May%202018.pdf Date of access: 18 May 2018.

Lewin, R. 1981. A signal intelligence war. *Journal of Contemporary History,* 16:501–512.

Liaropoulos, A. 2013. The challenges of social media intelligence for the intelligence community. *Journal of Mediterranean and Balkan Intelligence*, January:5–14.

Ling, J. 2017. Monitoring your memes. https://news.vice.com/en_ca/article/nedxez/the-canadian-government-developed-software-to-monitor-your-social-media-for-threats Date of access: 18 May 2018.

Lister, M., Dovey, J., Giddings, S., Grant, I. & Kelly, K. 2003. New media: A critical introduction. Oxon: Routledge.

Liu, W., Valente, T. & Beacom, A.M. 2017. Social network theory. https://www.researchgate.net/profile/Thomas_Valente/publication/316250457_Social_Network_Theory/links/59cca8c8a6fdcc451d61779f/Social-Network-Theory.pdf?origin=publication_detail Date of access: 25 Jun. 2018.

Lombardi, M., Rosenblum, T. & Burato, A. 2016. From SOCMINT to HUMINT: re-frame the use of social media within the intelligence cycle. www.fondaziodegasperi.org/wp-content/uploads/2016/04/socmint-humint.pdf Date of access: 13 Aug. 2017.

Lowenthal, M.M. 2006. Intelligence: From secrets to policy. Washington: CQ Press.

Mahlase, M. 2018. Analysts divided as Ramaphosa brings back Mbeki securocrats to probe State Security Agency. https://www.news24.com/SouthAfrica/News/analysts-divided-as-ramaphosa-brings-back-mbeki-securocrats-to-probe-state-security-agency-20180615 Date of access: 14 Aug. 2018.

Malcolm, J. 2013. Internet freedom in a world of states. http://www.intgovforum.org/cms/wks2013/workshop_background_paper/64_1367863304.pdf Date of access: 22 Apr. 2018.

Many Possibilities. 2014. African undersea cables. http://www.manypossibilities.net/african-undersea-cables/ Date of access: 14 Apr. 2014.

Marais, N. 2018. Ramaphosa will need to tackle the State Security Agency. https://www.dailymaverick.co.za/opinionista/2018-02-05-ramaphosa-will-need-to-tackle-the-state-security-agency/ Date of access: 18 May 2018.

Marcellino, W., Smith, M.L., Paul, C. & Skrabala, L. 2017. Monitoring social media: lessons for future Department of Defence social media analysis in support of information operations. www.rand.org/t/rr1742 Date of access: 10 May 2018.

Marchetti-Bowick, M. & Chambers, N. 2012. Learning for microblogs with distant supervision: political forecasting with Twitter. Delivery.acm.org/10.1145/2390000/2380890/p603-marchetti-bowick.pdf? Date of access: 27 Aug. 2017.

Marin, V. 2007. Public relations – content and models. http://www.afahc.ro/ro/revista/Nr_1_2007/Art_Marin.pdf Date of access: 6 Aug. 2018.

Marrin, A. 2014. Improving intelligence studies as an academic discipline. *Intelligence and National Security*, October:1–14.

Marsh, D. & Furlong, P. 2002. A skin, not a sweater: ontology and epistemology in political science. (*In* Marsh, D. & Stoker, G., *eds*. Theory and methods in political science. Hampshire: Palgrave Macmillan. p. 17–41).

Marshall, P. 2012. Don't look now, but everybody (CIA, DHS, etc.) is watching. https://gcn.com/Articles/2012/04/02/Social-media-analytics-hits-privacy-line.aspx?p=1 Date of access: 18 May 2018.

Maseko, F. 2016. South Africa: Social media reacts to #FeesMustFall as students protest. http://www.itnewsafrica.com/2016/09/south-africa-social-media-reacts-to-feesmustfall-as-student-protest/ Date of access: 18 May 2018.

Matey, G.D. 2005. Intelligence studies at the dawn of the 21st century: new possibilities and resources for a recent topic in international relations. https://www.ucm.es>www>Gustavo2 Date of access: 21 Mar. 2016.

Mayfield, A. 2008. What is social media? http://www.icrossing.com/uk/sites/default/files_uk/insight_pdf_files/What%20is%20Social%20Media_iCrossing_ebook.pdf Date of access: 18 Apr. 2018.

McQuail, D. 2010. Mass communication theory. London: Sage.

McQuail, D. 2013. Reflections on paradigm change in communication theory and research. *International journal of communication*, 7:216–229.

McSweeney, B. 2004. Security identity and interests: A sociology of international relations. New York: Cambridge University Press.

Mearsheimer, J. 2007. Structural realism. (*In* Dunn, T. & Kurki, M., *eds*. International relations theories: discipline and diversity. New York: Oxford University Press. p. 71–88.)

Meola, A. 2016. What is the internet of things (IoT)? Business Insider. http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8 Date of access: 25 Jan. 2017.

Merriam-Webster Dictionary. 2004. Social media. https://www.merriam-webster.com/dictionary/social%20media Date of access: 21 Aug. 2017.

Merriam-Webster Dictionary. 2018. Social network. https://www.merriam-webster.com/dictionary/social%20network Date of access: 24 Apr. 2018.

Meyer, H.M. 1987. Real world intelligence. New York: Weidenfeld & Nicolson.

Miles, M. & Huberman, A. 1994. Qualitative data analysis: an expanded sourcebook. Thousand Oaks: Sage Publications.

Miller, B.H. 2008. Improving all source intelligence analysis: elevate knowledge in the equation. *International Journal of Intelligence and Counter Intelligence,* 21(2):337–354.

Moe, W.W. & Schweidel, D.A. 2014. Social media intelligence. Cambridge: Cambridge University Press.

Montagnese, C.C.A. 2012. Impact of social media on national security. http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Documents/Ricerche/2012/Stepi/social_media_20120313_0856.pdf Date of access: 9 Aug. 2017.

Mora, J. 2012. The analysis of interactive media and digital culture: hypermedia literacy in Peru and Bolivia. *Comunicar Journal*, 39(XX):139–149.

Moreau, E. 2018. What does it mean to go viral online? https://www.lifewire.com/what-does-it-mean-to-go-viral-3486225 Date of access: 1 May 2018.

Morozov, E. 2011. The net delusion: the dark side of internet freedom. New York: Public Affairs.

Mostert, J. 2017. The use of technology in NIS [personal interview]. 17 Jul., Pretoria.

Mouton, J. 2007. Understanding social research. Pretoria: Van Schaik Publishers.

Mouton, J. 2011. How to succeed in your master's and doctoral studies. Pretoria: Van Schaik.

Mouton, J. & Marais, H. 1996. Basic concepts in the methodology of the social sciences. Pretoria: HSRC Publishers.

Mozaffari, A. & Posno, A. 2016. Outcry may curtail police social media surveillance. https://www.thelawyersdaily.ca/articles/3685/outcry-may-curtail-police-social-media-surveillance Date of access: 31 May 2018.

Mulambo, J.R. 2017. The power of Twitter and Facebook in democracy. www.news24.com/MyNews24/the-power-of-twitter-and-facebook-at-the-heart-of-democratic-crisis-20170411 Date of access: 10 May 2018.

Mungiu-Pippidi, A. & Munteanu, I. 2009. Moldova's "Twitter revolution". *Journal of Democracy*, 20(3):136–142.

Murray, W. 2002. World War II: Ultra – The misunderstood allied secret weapon. http://www.historynet.com/world-war-ii-ultra-the-misunderstood-allied-secret-weapon.htm Date of access: 11 Jan. 2017.

Nathan, L. 2012a. A critique of the General Intelligence Laws Amendment Bill. http://www.politicsweb.co.za/documents/a-critique-of-the-general-intelligence-laws-amendm Date of access: 29 May 2018.

Nathan, L. 2012b. Tool 3: Intelligence transparency, secrecy and oversight in a democracy. (*In* Born, H. & Wills, A *eds*. Overseeing intelligence services: A toolkit. Geneva: Centre for the Democratic control of armed forces. p. 49–68).

National Strategic Intelligence Act **see** South Africa.

Neuman, W. 2006. Basics of social research: qualitative and quantitative approaches. Boston: Allyn and Bacon.

Neuman, W.R. 2008. Interactivity, concept of. (*In* Donsbach, W., *ed*. The international encyclopedia of communication. Malden: Blackwell. p. 2318–2322).

Newme, K. 2011. Traditional media, meaning and practices. shodhganga.inflibnet.ac.in/bitstream/10603/97789/5/ch3.pdf Date of access: 23 Jun. 2018.

Ngai, E.W.T., Tao, C.S. & Moon, K.K.L. 2015. Social media research: theories, constructs, and conceptual frameworks. *International Journal of Information Management*, 35(1):33–44.

NIC (National Intelligence Council). 2007. Non-state actors: impact on international relations and implications for the United States. https://www.dni.gov/files/documents/nonstate_actors_2007.pdf Date of access: 19 Mar. 2015.

NIC (National Intelligence Council). 2012. Global trends: Alternative worlds. https://gloabltrends2030.files.worlpress.com/2012/11/global-trends-2030-november2012.pdf Date of access: 8 Aug. 2015.

Nielsen. 2012. State of the media: The social media report. https://www.nielsen.com/in/en/insights/reports/2012/state-of-the-media-the-social-media-report-2012.html Date of access: 14 Jan. 2014.

Novikov, D.A. 2016. Cybernetics: past to future. https://www.researchgate.net/profile/Dmitry_Novikov5/publication/287319297_Cybernetics_from_Past_to_Future/links/56754f8208ae125516e6fff3/Cybernetics-from-Past-to-Future.pdf?origin=publication_detail Date of access: 15 Jul. 2018.

NSTI (National Security Training Institute). 2012. The effects of social media on national security. nstii.com/content/effects-social-media-national-security-part-1 Date of access: 17 Feb. 2014.

Nye, J.S. Jr. & Lynn-Jones, S.M. 1988. International security studies: a report of a conference on the state of the field. *International Security*, 12(4):5–27.

O'Brien, K. 2011. The South African intelligence services: From apartheid to democracy 1948–2005. Abington: Routledge.

OECD (Organisation for Economic Co-operation and Development). 2014. https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf Date of access: 19 Apr. 2018.

Omand, D. 2013. Social media: the security challenge. https://m.youtube.com/watch?v=q-bn752l-ba Date of access: 31 Aug. 2017. [Youtube].

Omand, D., Bartlett D. & Miller, C. 2012a. Introducing social media intelligence (SOCMINT), *Intelligence and national security journal*, 27(6):801-823.

Omand, D., Bartlett, J. & Miller, C. 2012b. #Intelligence. https://www.demos.co.uk?wp-content/uploads/2017/03/intelligence-report.pdf Date of access: 18 Aug. 2017.

Omand, D., Bartlett D. & Miller, C. 2014. Towards the discipline of social media intelligence. (*In* Hobbs, C., Moran, M. & Salisbury, D., *eds*. Open source intelligence in the twenty first century: new approaches and opportunities. Hampshire: Macmillan. p. 24–43).

Omand, D. & Phythian, M. 2012. Ethics and intelligence: a debate. *International Journal of Intelligence and Counter Intelligence*, 26(1):38–63.

Omede, A.J. 2015. Social media: a trend or threat to democracy. *Jorind*, 13(1):272–278. www.transcampus.org/jorindv13jun2015/jorind%20vol13%20no1%20jun%20chapter31.pdf Date of access: 16 Aug. 2017.

Orbe, M.P. 2009. Phenomenology. (*In* Littlejohn, S.W. & Foss, K.A., *eds*. Encyclopedia of communication theory. Thousand Oaks: Sage. p. 749–751).

Orihuela, J.L. 2003. eCommunication: the 10 paradigms of media in the digital age. https://www.slideshare.net/jlori/orihuela-cost-paper Date of access: 6 Aug. 2017.

Oxford Martin School. 2013. Now for the long term. http://www.oxfordmartin.ox.ac.uk/Oxford_Martin_Now_for_the_Long_Term Date of access: 31 Oct. 2013.

Padmakumara, S.C. 2014. The disciplinary identity of IR: an analysis on cross disciplinary enterprise. *International Journal of Scientific Research and Innovative Technology,* 1(5):83–92.

Papic, M. & Noonan, S. 2011. Social media as a tool for protest. http://dalpemilette.com/files/pdf/infosabius/2011_03/InfoSabius_2-11_03_07_MediasSociaux.pdf Date of access: 23 Aug. 2017.

Parcell, L.M. 2008. Communication and media studies: history since 1968. (*In* Donsbach, W., *ed*. The international encyclopedia of communication. Malden: Blackwell. p. 757–764).

Perrons, D. 2004. Globalization and social change: people and places in a divided world. London: Routledge.

Phythian, M. 2009. Intelligence theory and theories of international relations: Shared world or separate worlds. (*In* Gill, P., Marrin, S. & Phythian, M., *eds*. Intelligence theory. Key questions and debates. New York: Routledge. p. 54–72).

Pirsig, R.M. 2012. The psychology of social. https://www.slideshare.net/StevenDuque/amp-agency-the-psychology-of-social-february-2012 Date of access: 27 Apr. 2018.

Popper, K. 2002. The logic of scientific discovery. New York: Routledge.

Potts, D.A. 2014. Characteristics of the internet. http://www.cyberlibel.com?p=1132 Date of access: 12 Apr. 2018.

Promotion of access to information Act **see** South Africa.

Public Protector South Africa. 2016. State of capture. Saflii.org/images/329756472-state-of-capture.pdf Date of access: 12 Oct. 2017.

Quan-Haase, A. & Young, A.L. 2010. Uses and gratifications of social media: a comparison of Facebook and Instant Messaging. *Bulletin of Science Technology & Society*, 30(5):350–361.

Rafaeli, S. 1988. Interactivity: from new media to communication. *Sage annual review of communication research: Advancing communication Science*, 16:110–134.

Rathmell, A. 2002. Towards postmodern intelligence. *Intelligence and National Security Journal*, 17(3):87–104.

Ravitch, S.M. & Riggan, J.M. 2017. Reason and rigor how conceptual frameworks guide research. Thousand Oaks: Sage Publications.

Rennie, S. 2013. Social media to be monitored by federal government. https://www.thestar.com/news/canada/2013/11/29/social_media_to_be_monitored_by_federal_government.html Date of access: 18 May 2018.

RICA (Regulation of Interceptions of Communications and Provision of Communication - Related information) **see** South Africa.

Rickli, J. & Kaspersen, A. 2016. The global war of narratives and the role of social media. https://www.weforum.org/agenda/2016/07/the-global-war-of-narratives-and-the-role-of-social-media/ Date of access: 11 May 2018.

Right2Know. 2018. About. http://www.r2k.org.za/about/ Date of access: 18 May 2018.

Risjord, M. 2014. Philosophy of social science: a contemporary introduction. New York: Routledge.

Rogers, T. 2018. Understanding citizen journalism: the power and perils of independent reporting. https://www.thoughtco.com/what-is-citizen-journalism-2073663 Date of access: 6 Nov. 2018.

Rothschild, E. 1995. What is security? *Daedalus*, 124(3):53–98.

Rovner, J. 2013. Intelligence in the Twitter age. *International Journal of Intelligence and Counter Intelligence,* 26(2):260–271.

Ruggiero, T.E. 2000. Uses and gratification theory in the 21st century. *Mass Communication and Society*, 3(1):3–37.

Ryan, J. 2010. A history of the Internet and the digital future. London: Reaction Books.

Safko, L. 2012. The social media bible: Tactics, tools & strategies for business success. Hoboken: John Wiley & Sons.

Safranek, R. 2012. The emerging role of social media in political and regime change. www.csa.com/discoveryguides/discoveryguides-main.php Date of access: 16 Aug. 2017.

Salaverria, R. 2017. Typology of digital news media: theoretical bases for their classification. *Mediterranean Journal of Communication*, 8(1):19–32.

Sanders, J. 2006. Apartheid's friends: the rise and fall of South Africa's Secret Service. London: John Murray Publishers.

Sangham, M. 2017. From fees must fall To Zuma must fall: What 1.4M Tweets say about the future of South Africa. https://www.thedailyvox.co.za/fees-must-fall-zuma-must-fall-1-4m-tweets-say-future-south-africa/ Date of access: 18 May 2018.

SAPS (South African Police Service). 2010. Strategic Plan 2010–2014. https://www.saps.gov.za/about/stratframework/strategic_plan/2010_2014/strategic_plan_2010_2014.pdf Date of access: 18 May 2018.

SAPS ***see*** South African Police Service.

SAS. 2012. Using intelligence from social media to combat security threats. Medmenham: SAS Institute.

Saunders, M., Lewis, P. & Thornhill, A. 2012. Research methods for business students. Essex: Pearson Education.

Sayer, A. 1992. Methods in social science: a realist approach. New York: Routledge.

Schein, R., Wilson, K. & Keelan, J. 2010. Literature review on effectiveness of the use of social media: a report for Peel Public Health. www.peelregion.ca/health/resources/pdf/socialmedia.pdf Date of access: 8 Aug. 2017.

Schram, M. 2018. The big battle: social media vs. social networking. https://www.cmnty.com/blog/social-media-vs-social-networking/ Date of access: 27 Apr. 2018.

Schwab, K. 2016. The fourth industrial revolution. Genève: World Economic Forum.

Scolari, C. 2009. Mapping conversations about new media: the theoretical field of digital communication. http://nms.sagepub.com/cgi/content/abstract/11/6/943 Date of access: 10 Jan. 2015.

Scott, J. 2000. Social network analysis: a handbook. London: Sage

Scott, L. & Jackson, P. 2004. The study of intelligence in theory and practice. *Intelligence and National Security Journal*, 19(2):139–169.

Scott, P. & Jacka, J. 2011. Auditing social media – governance and risk guide. Hoboken: Hoboken Wiley.

Sevenzo, F. 2017. Kenya election: Fake CNN, BBC reports target voters. CNN, 1 Aug. edition.cnn.com/2017/07/31/Africa/Kenya-elections-fake-news/index.html Date of access: 24 Aug. 2017.

Sheehan, M., *ed*. 2000. National and international security. Burlington: Ashgate Publishing Company.

Sheldon, R.M. 2003. Intelligence in the ancient world. http://wwwrieas.gr/images/profsheldon.pdf Date of access: 21 Mar. 2016.

Shepherd, L.J. 2013. Critical approach to security. Abington: Routledge.

Sherry, J.L. & Boyan, A. 2008. Uses and gratifications. (*In* Donsbach, W., *ed*. The international encyclopedia of communication. Malden: Blackwell. p. 5239–5244).

Shirky, C. 2011. The political power of social media. *Foreign Affairs,* 13(2):1–9.

Shullich, R. 2011. Risk assessment of social media. http://www.sans.org/reading-room/risk-assessment-social-meida-33940 Date of access: 4 Jun. 2013.

Shulsky, A.N. 1995. What is intelligence? Secret and competition among states. (*In* Godson, R., May, E. & Schmitt, G., *eds*. US intelligence at the crossroads. Washington: Brassey's. p. 17–27).

Shulsky, A.N. & Schmitt, G.T. 2002. Silent warfare: Understanding the world of intelligence. Dulles: Potomac Books.

Simonson, P. & Peters, J.D. 2008. Communication and media studies: history to 1968. (*In* Donsbach, W., *ed*. The international encyclopedia of communication. Malden: Blackwell. p. 764–771).

Sims, J. 1995. What is intelligence? Information for decision makers. (*In* Godson, R., May, E. & Schmitt, G., *eds*. US intelligence at the crossroads. Washington: Brassey's. p. 3–16).

Sims, J. 2009. Defending adaptive realism: intelligence theory comes of age. (*In* Gill, P., Marrin, S. & Phythian, M., *eds*. Intelligence theory. Key questions and debates. New York: Routledge. p. 151–165).

Sipalan, J. 2018. Malaysia outlaws 'fake news'; sets jail of up to six years. https://www.usnews.com/news/world/articles/2018-04-02/malaysia-outlaws-fake-news-sets-jail-of-up-to-six-years Date of access: 18 May 2018.

Snow, D.M. 2014. National security for a new era. London: Routledge.

Söderblom, J. 2004. Opening the intelligence window: realist logic and the invasion of Iraq. *Perception*, Summer:21–1.

South Africa. 1983. Republic of South Africa Constitution Act 110 of 1983. https://law.wisc.edu/gls/cbsa2.pdf Date of access: 14 Aug. 2017.

South Africa. 1993. Transitional executive Council Act 151 of 1993.

South Africa. 1994a. Intelligence Services Oversight Act 40 of 1994.

South Africa. 1994b. National Strategic Intelligence Act 39 of 1994.

South Africa. 2000. Promotion of access to information Act 2 of 2000.

South Africa. 2002a. Defence Act 42 of 2002.

South Africa. 2002b. Electronic Communication Security (Pty) Ltd Act 68 of 2002.

South Africa. 2002c. Intelligence Services Act 65 of 2002.

South Africa. 2002d. Regulation of Interceptions of Communications and Provision of Communication - Related information (RICA) Act 70 of 2002.

South Africa. 2008. Intelligence Services Amendment Bill B37-2008.

South Africa. 2009a. Administration and operations – Government Component: National Intelligence Agency. (Notice 912). *Government Gazette*, 32576:7, 17 Sept.

South Africa. 2009b. Administration and operations – Government Component: South African Secret Service. (Notice 913). *Government Gazette*, 32576:7, 17 Sept.

South Africa. 2009c. Administration and operations – Government Component: Intelligence Academy. (Notice 914). *Government Gazette*, 32576:11, 17 Sept.

South Africa. 2009d. Administration and operations – Government Component: COMSEC. (Notice 915). *Government Gazette*, 32576:15, 17 Sept.

South Africa. 2013. General Intelligence Laws Amendment Act 11 of 2013. Pretoria: Government Printer.

South Africa. 2017. Cybercrime and cybersecurity bill. www.justice.gov.za/legislation/bills/cybercrimesbill2017.pdf Date of access: 25 Nov. 2017.

South Africa. Department of Justice. 1996. Statement to the Truth and Reconciliation Commission. http://www.justice.gov.za/trc/hrvtrans/submit/anctruth.htm Date of access: 4 Dec. 2017.

South Africa. Department of Justice. 1997. Further submissions and responses by the African National Congress to questions raised by the commission for truth and reconciliation. http://www.justice.gov.za/trc/hrvtrans/submit/anc2.htm Date of access: 22 Jun. 2017.

South Africa. 1995. White Paper on Intelligence.

South Africa. 1996. Constitution of the Republic of South Africa.

South Africa. State Security Agency. 2018. President Ramaphosa appoints high-level review panel on State Security Agency. http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2018/President%20appoints%20review%20panel_15June2018.pdf Date of access: 10 Aug. 2018.

South African History Online. 2011a. Hendrik Frensch Verwoerd. https://www.sahistory.org.za/people/hendrik-frensch-verwoerd Date of access: 16 Sept. 2018.

South African History Online. 2011b. The homelands. https://www.sahistory.org.za/article/homelands Date of access: 16 Sept. 2018.

South African History Online. 2016a. The South African BOSS is established. www.sahistory.org.za/dated-event/south-african-bureau-boss-established Date of access: 26 Apr. 2017.

South African History Online. 2016b. A white referendum. www.sahistory.org.za/articel/white-referendum Date of access: 18 Jun. 2017.

State Security Agency ***see*** South Africa. State Security Agency.

Statista. 2018. Most famous social media network sites worldwide as of July 2018. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ Date of access: 5 Sept. 2018.

Steinitz, C. & Zarin, H. 2012. An initial look at the utility of social media as a foreign policy tool. https://www.cna.org?cna_files/pdf?dop-2012-u-002538-final.pdf Date of access: 14 Aug. 2017.

Suchý, P. 2003. Role of security and strategic studies within international relations studies. www.mocr.army.cz/mo/obrana_a_strategic/2-2003eng/suchy.pdf Date of access: 30 Jul. 2014.

Sulick, M. 2014. Intelligence in the Cold War. *The Intelligencer,* 21(1):47–52.

Svantesson, D.J.B. 2006. The not so “borderless” internet: Does it still give rise to private international law issues? http://epublications.bond.edu.au/law_pubs/96 Date of access: 22 Apr. 2018.

Swanepoel, P.C. 2007. Really inside BOSS: A tale of South Africa’s late intelligence service (And something about the CIA). Derdepoortpark: Imprint.

Swart, H. 2011. Secret state: How the government spies on you. http://amabhungane.co.za/article/2011-10-14-secret-state Date of access: 20 May 2018.

Swart, H. 2015. Big Brother is listening – on your phone. https://mg.co.za/article/2015-11-12-big-brother-is-listening-on-your-phone Date of access: 18 May 2018.

Swart, H. 2016. Communication surveillance by the South African intelligence services. http://www.mediaandemocracy.com/uploads/1/6/5/7/16577624/comms-surveilance-nia-swart feb2016.pdf Date of access: 7 Jun. 2017.

Swart, H. 2017. Big Brother is watching your phone call records. https://www.dailymaverick.co.za/article/2017-05-10-op-ed-big-brother-is-watching-your-phone-call-records/#.WwFdce6FOM8 Date of access: 18 May 2018.

Swart, H. 2018. Government surveillance of social media is rife. Guess who's selling your data? https://www.dailymaverick.co.za/article/2018-04-25-government-surveillance-of-social-media-is-rife-guess-whos-selling-your-data/#.WvmUl6SFOM8 Date of access: 18 May 2018.

Tannam, E. 2017. British intelligence allegedly using social media for mass surveillance. https://www.siliconrepublic.com/enterprise/uk-social-media-surveillance Date of access: 18 May 2018.

Teitelbaum, L. 2004. The impact of the information revolution on policymakers' use of intelligence analysis. Santa Monica: Pardee Rand Graduate School. (Thesis – PhD).

Tenet, G. J. 2010. The CIA and the security challenges of the new century. *International Journal of Intelligence and Counter Intelligence,* 13(2):133–143.

Terre Blanche, M., Durrheim, K. & Painter, D. 2012. Research in practice: applied methods for the social sciences. Cape Town: University of Cape Town Press.

Testa, A. 2018. Analysis: How Bell Pottinger met its end in South Africa. https://www.iol.co.za/business-report/companies/analysis-how-bell-pottinger-met-its-end-in-south-africa-13127573 Date of access: 20 May 2018.

Theohary, C. & Rollins, J. 2011. Terrorist use of the internet: information operations in cyberspace. www.fas.org/sgp/crs/terror/R41674.pdf Date of access: 18 Feb. 2014.

Thomas, L. 2003. Al Qaeda and the internet: the danger of "cyberplanning". www.strategicstrudiesinstitute.army.mil/pubs/parameters/articles/thomas.pdf Date of access: 6 Feb. 2014.

Thomas, S. 2015. #FeesMustFall: how SA students are using social to subvert traditional media. https://memeburn.com/2015/10/feesmustfall-how-sas-students-are-using-social-to-subvert-traditional-media-narratives/ Date of access: 16 May 2018.

Thomas, S.T. 1988. Assessing current intelligence studies. *Intelligence and Counterintelligence*, 2(2):217–244.

Thompson, R. 2011. Radicalization and the use of social media. *Journal of strategic security*, 4(4):167–190.

Toffler, A. 1990. Powershift: Knowledge, wealth and violence at the edge of the 21st century. New York: Bantam Books.

Trading Economics. 2018. South Africa youth unemployment rate. https://tradingeconomics.com/south-africa/youth-enemplyment-rate Date of access: May 2018.

Transitional executive Council Act **see** South Africa.

Treverton, G. 2011. Reshaping intelligence for an age of terror: Where do we stand? Web.mit.edu/ssp/seminars/wed_archives_2011Spring/treverton.html Date of access: 17 Feb. 2014.

Treverton, G.F., Jones, S.G., Boraz, S. & Lipscy, P. 2006. Towards a theory of intelligence: Workshop report. https://www.rand.org/content/dam/rand/pubs/conf_proceedings/2006/rand_cf219.pdf Date of access: 20 Jan. 2014.

Troy, T.F. 1991. The "correct" definition of intelligence. *International Journal of Intelligence and Counterintelligence,* 5(4):433–454.

Turck, L. 2016. An investigation into the utilisation of social media by the SAPS in resolving crimes. Pretoria: UNISA. (Dissertation – Masters).

Ullman, R. 1983. Redefining security. *International Security,* 8(1):129–153.

Umraw, A. 2017. How Bell Pottinger's Gupta campaign damaged South Africa. Huffpost, 7 July. www.huffingtonpost.co.za/2017/07/07/how-bell-pottingers-gupta-campaign-damaged-south-africa_a_23020707/ Date of access: 24 Aug. 2017.

Ungerer, C. 2012. Introductory paper. (*In* ASPI Strategic policy form: Topic: Social media and national security. Australian Strategic Policy Institute. p. 1).

Van De Ven, A. 2007. Engaged scholarship: a guide for organisational and social research. New York: Oxford University Press.

Van Den Berg, M.A. 2014. Intelligence regimes in South Africa (1994–2014): and analytical perspective. Potchefstroom: North-West University. (Thesis – Masters).

Van Den Berg, M.A. 2018. Intelligence practices in South Africa as hybrid political regime: a meta-theoretical and theoretical analysis. Potchefstroom: North-West Univeristy. (Thesis – PhD).

Van Der Merwe, M. 2017. State Security and social media: Is big brother following you? Daily Maverick. https://www.dailymaverick.co.za/article/2017-03-07-state-security-and-social-media-is-big-brother-following-you/ Date of access: 17 Oct. 2017.

Van Der Waag, I. 2015. A military history of modern South Africa. Jeppestown: Jonathan Ball Publishers.

Van Rheede van Oudtshoorn, G.P. 2011. 7 Metateoretiese tradisies teoretiese benaderings. A lecture at the North West University. [PowerPoint Presentation].

Van Solms, B. 2014. Basie Van Solms: Offence the best form of defence. ITWeb, 29 May. www.itweb.co.za/index.php?option=com_content&view=article&id=134903 Date of access: 17 Mar. 2017.

Vetromedia. 2018. A glimpse at South Africa's social media landscape in 2018. http://www.vetro.co.za/2018/01/31/south-africas-social-media-landscape/ Date of access: 5 Sept. 2018.

Vidal, C. 2008. What is a worldview? (*In* Van Belle, H. & Van der Veken, J., *eds*. Niewheid denken. De wetenschappen en het creative aspect van de werklijheid. Acco: Leuven. p. 1–13).

Viotti, P. & Kauppi, M. 1999. International relations theory: realism, pluralism, globalisation and beyond. Needham Heights: Allyn & Bacon.

Wallis, S. 2010. Towards a science of metatheory. *Integral Review*, 6(3):73–120.

Walsh, P.F. 2011. Intelligence and intelligence analysis. Oxon: Routledge.

Walsh, P.F. 2014. Building better intelligence frameworks through effective governance. *International Journal of Intelligence and Counter Intelligence,* 28(1):123–142.

Walt, S. 1991. The renaissance of security studies. *International Studies Quarterly*, 35(2):211–239.

Waltz, K. 1979. Theory of international politics. Menlo Park: Addison-Wesley Publishing Company.

Wark, W.K., *ed.* 1994. Espionage: past, present and future? Oxon: Frank Cass & Co.

Wark, W.K. 2003. Introduction: Learning to live with intelligence. *Intelligence and National Security,* 18(4):1–14.

Warner, M. 2002. Wanted: a definition of "intelligence". *Studies in Intelligence,* 46(3):15–22.

Warner, M. 2009. Intelligence as risk shifting. (*In* Gill, P., Marrin, S. & Phythian, M., *eds*. Intelligence theory: Key questions and debates. New York: Routledge. p16–32).

We Are Social & Hootsuite. 2018. Digital in 2018. https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018 Date of access: 30 Apr. 2018.

Webopedia. 2007. Brief timeline of the internet. www.webopedia.com/quick_ref/timeline.asp Date of access: 9 Aug. 2017.

Weimann, G. 2004. How modern terrorism uses the internet. www.securityaffairs.org/issues/2005/08/weimannpdp Date of access: 6 Feb. 2014.

West, R. & Turner, L.H. 2010. Introducing communication theory: analysis application. New York: McGraw-Hill.

Wettering, F.L. 2001. The internet and the spy business. *International Journal of Intelligence and Counterintelligence*, 14(3):342–365.

White Paper on Intelligence **see** South Africa.

Whiting, A. & Williams, D. 2013. Why people use social media: a uses and gratification approach. https://www.researchgate.net/publication/237566776 Date of access: 14 Jul. 2018.

Wiener, J. & Schrire, R.A., *eds*. 2009. Encyclopaedia of life support systems: Volume 1. www.eolss.net Date of access: 13 Dec. 2015.

Wiener, N. 1961. Cybernetics: or control and communication in the animal and the machine. Cambridge: The MIT Press.

Wiggill, M.N. 2009. Strategic communication management in the non-profit adult literacy sector. Potchefstroom: North-West University. (Thesis – PhD).

Williams, F., Rice, R.E. & Rogers, E. 1988. Research methods and the new media. New York: Free Press.

Williams, M. & May, T. 2003. Introduction to the philosophy of social research. London: UCL Press.

Williams, M.L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., Morgan, J. & Sloan, L. 2013. Policing cyber-neighbourhoods: tension monitoring and social media networks. *Policing and Society: An International Journal of Research and Policy,* 23(4):461–481.

Williams, P., *ed*. 2008. Security studies an introduction. New York: Routledge.

Williams, R. 2000. The other armies: A brief historical overview of Umkhonto We Sizwe (MK), 1961–1994. *Military History Journal*, 11(5). www.samilitaryhistory.org/vol115rw.html. Date of access: 22 Jun. 2017.

Withers, I. 2017. Bell Pottinger kicked out of PR trade body as report slams 'race hate' South Africa campaign. *The Telegraph*, 17 Sept. http://www.telegraph.co.uk/business/2017/09/04/bell-pottinger-kicked-pr-trade-body-report-slams-race-hate-south/ Date of access: 6 Dec. 2017.

Wolfers, A. 1952. “National security” as an ambiguous symbol. *Political Science Quarterly*, 67(4):481–02.

World Economic Forum. 2017. The global risk report. 12th ed. www3.weforum.org/docs/grr17_report_web.pdf Date of access: 25 Nov. 2017.

Worley, D.R. 2015. Orchestrating the instruments of power: a critical examination of the US National Security System. Nebraska: University of Nebraska Press.

Wright, P. 2013. Meet Prism's little brother: Socmint. http://www.wired.co.uk/article/socmint Date of access: 28 May 2018.

Writer, S. 2014. Social media in defence intelligence gathering. http://www.defenceweb.co.za/index.php?option=com_content&task=view&id=34477&Itemid=242 Date of access: 29 May 2018.

Writer, S. 2017. Bell Pottinger white monopoly capital plot: Damning evidence of Gupta conspiracy #GuptaLeaks. https://www.biznews.com/guptaleaks/2017/06/09/bell-pottinger-white-monopoly-capital/ Date of access: 18 May 2018.

Writer, S. 2018. Government wants to change laws that allow for “mass spying” on SA phones. https://businesstech.co.za/news/technology/230797/government-wants-to-change-laws-that-allow-for-mass-spying-on-sa-phones/ Date of access: 18 May 2018.

Wu, P. 2015. Impossible to regulate: social media, terrorists and the role of the U.N. *Chicago Journal of International Law*, 16(1). http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1690&context=cjil Date of access: 17 Oct. 2017.

APPENDIX – DECLARATION OF LANGUAGE EDITING

cumlaude
language practitioners

Director: CME Terblanche - BA (Pol Sc), BA Hons (Eng), MA (Eng), TEFL

22 Strydom Street
Baillie Park, 2531

Tel 082 821 3083
cumlaudelanguage@gmail.com

DECLARATION OF LANGUAGE EDITING

I, Christina Maria Etrecia Terblanche, hereby declare that I edited the research study titled:

Social media intelligence (SOCMINT) within the South African context: A theoretical and strategic framework for the national security environment

for **JI Stegen** for the purpose of submission as a postgraduate study for examination. Changes were indicated in track changes and implementation was left to the author.

Regards,

CME Terblanche

Cum Laude Language Practitioners (CC)

SATI accreditation no: 1001066 (South African Translators Institute)

Full member of PEG (Professional Editor's Guild)