

https://dspace.org/

Investigating the Challenges of Adopting Social Media Intelligence (SOCMINT) as a Tool for Mitigating National Security Threats in South Africa – The July 2021 Unrest Case Study

Rikhotso, Bridget Vulani

2025

University of the Witwatersrand, Johannesburg

https://hdl.handle.net/10539/50139

Rikhotso, Bridget Vulani . (2025). Investigating the Challenges of Adopting Social Media Intelligence (SOCMINT) as a Tool for Mitigating National Security Threats in South Africa – The July 2021 Unrest Case Study [Master's dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/50139

Downloaded from a DSpace repository. https://dspace.org/



UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

Investigating the Challenges of Adopting Social Media Intelligence (SOCMINT) as a Tool for Mitigating National Security Threats in South Africa – The July 2021 Unrest Case Study

RESEARCH REPORT

Submitted in fulfillment of the requirements for the degree of Master of Commerce (MCom) by Research in the field of Information Systems

School of Business Sciences Faculty of Commerce, Law and Management University of the Witwatersrand, Johannesburg, South Africa

By

Bridget Vulani Rikhotso

Student Number: 2514770

Supervisor: Dr. Kebashnee Moodley

DECLARATION

I certify that this is my original work and that all references to outside sources have been appropriately and completely acknowledged.

BV RIKHOTSO



ACKNOWLEDGEMENTS

I would like to give thanks to the Lord, who has given be wisdom, strength and a sound mind during this research project.

My sincere gratitude to my supervisor Dr. Kebashnee Moodley for the continuous support of my Master's degree. I appreciate her motivation, patience and immense knowledge. I thank her for always being available and providing valuable feedback.

Great thanks to my employer for allowing me further my studies and to conduct the qualitative case study onsite.

ABSTRACT

The purpose of this study was to examine the challenges faced by the South African intelligence community in adopting Social Media Intelligence (SOCMINT) as a tool for mitigating national security threats, particularly in light of the failure to predict the July 2021 civil unrest. As we enter the Fourth Industrial Revolution (4IR), technological innovations are reshaping the intelligence collection landscape, with social media technologies offering new methods for addressing national security concerns. Despite the significance of SOCMINT, the South African intelligence agencies have not fully embraced this discipline, contributing to one of the nation's major intelligence failures.

While the driving forces and consequences of the July 2021 unrest have been extensively analysed, the reasons behind the intelligence agencies' inability to anticipate it remains underexplored. This interpretive study aimed to uncover these challenges, guided by the Technology-Organisation-Environment (TOE) framework integrated with the Unified Theory of Acceptance and Use of Technology (UTAUT). Data was collected from intelligence experts and analysts to provide a comprehensive perspective on the issue. A single organisation case study approach was adopted to achieve a deeper understanding of the phenomenon within the intelligence community.

This study developed an integrated conceptual framework underpinned by the Technology Organisation Environment (TOE) framework and UTAUT Theory. This integrated framework was used to investigate the challenges that hinder the adoption of SOCMINT through a qualitative case study that was conducted in the South African intelligence community. Data for this research was collected from twelve participants representing operations, IT, analysts, and management. Findings revealed that the major challenges experienced are more organisational (Management support, Technology Inclination and Cost) and environmental (Silo, Government Regulations and Coordination) as factors of adoption. From the technological context, there were no major challenges highlighted with the exception of security. Other technological factors or challenges raised by participants, compatibility, expectancy, and performance, were unpersuasive and immaterial to the adoption of SOCMINT.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION 5
1. INTRODUCTION 5
1.1 Background 6
1.2 Contextualisation 8
1.3 Problem statement 10
1.4 Research questions 12
1.5 Research Objectives 12
1.6 Purpose of the study 13
1.7 Research lmitations 13
1.8 Intended contribution 14
1.9 Research Methodology Approach 15
1.10 Summary 17
CHAPTER 2: LITERATURE REVIEW **18**
2. INTRODUCTION 18
2.1 The role of intelligence and its application to national security 18
2.2 Sub-categories of Intelligence Communities 24
2.3 The effectiveness of SOCMINT as an intelligence collection discipline 25
2.4 Social media landscape 28
2.5 Social Media and its impact on national security 33
2.5.1 The international impact of social media to national security 33
2.5.2 The South African impact of social media on national security 35
2.5.3 South Africa's response to the July 2021 unrest 36
2.6 Lessons to be learnt from intelligence failures 39
2.7 SOCMINT Opportunities 40
2.8 SOCMINT as an intelligence collection method 42
2.9 SOCMINT Challenges 45
2.10 Legal, Ethical and Privacy consideration 46
2.11 Regulation of SOCMINT in South Africa 47
2.12 Theoretical Framework 49
2.12.1 Diffusion of Innovations 50
2.12.2 Technology Organisation-Environment (TOE) 51
2.12.3 The Unified Theory of Acceptance and Use of Technology (UTAUT) 52
2.13 Factors that influence technology adoption 53
2.13.1 Technology Factors 54

2.13.2 Organisation Factors 55
2.13.3 Environmental issues 56
2.13.4 Individual Factors 57
2.14 Integrated TOE and UTAUT Framework 58
2.15 Summary 59
CHAPTER 3: METHODOLOGY 60
3.1 INTRODUCTION 60
3.2 Research paradigm and approach 60
3.3 Research Design and Strategy 62
3.4 Case Study Approach 63
3.5 Time horizon 64
3.6 Data Collection Methods 64
3.7 Data Analysis Method 66
3.8 Ethical Consideration 67
3.9 Summary 68
CHAPTER 4: DATA ANALYSIS AND FINDINGS 70
4.1 INTRODUCTION 70
4.2 Participants 70
4.3 Interview Questions Profile and Response Rate 71
4.4 Documents Reviewed 72
4.5 Presentation and Findings 72
4.6 Summary 100
CHAPTER 5: DISCUSSION OF RESULTS 101
5. INTRODUCTION 101
5.1 Discussion of findings 101
5.2 Final Conceptual Framework for SOCMINT adoption 106
5.3 Research questions addressed in this study 107
5.5 Summary 111
CHAPTER 6: CONCLUSION 113
6.1 INTRODUCTION 113
6.2 Implications of this study 113
6.3 Recommendations 113
6.4 Future Research 115
REFERENCES 116
APPENDIX A: ETHICAL CLEARANCE CERTIFICATE 145
APPENDIX B: PARTICIPATION INFORMATION 146

APPENDIX C: INTERVIEW SCHEDULE **149**
APPENDIX D: ILLUSTRATION OF TRANSCRIBED INTERVIEW AND CODING **151**
APPENDIX E: LETTER OF PERMISSION FROM INTELLIGENCE COMMUNITY **153**
APPENDIX F: ILLUSTRATION OF CONSENT FORM **155**

LIST OF FIGURES

Figure 1 Intelligence Process (Lowenthal, 2022) 21
Figure 2 The most used social media platforms in South Africa (Business Tech, 2023) 31
Figure 3 top 12 accounts belonging to RET network (Mokoka, 2021) 37
Figure 4 The proposed conceptual framework 54
Figure 5 The research onion approach (Saunders et al., 2009) 60
Figure 6 Final Intergraded Conceptual Framework 106

LIST OF TABLES

Table 1 Significant mass demonstrations 33
Table 2 SOCMINT intelligence collection methods ..... **Error! Bookmark not defined.**
Table 3 Modern SOCMINT Technology 43
Table 4 Qualitative thematic analysis (Clarke & Braun, 2013) 66
Table 5 The following participants were interviewed 71
Table 6 Summary of Themes 73

LIST OF KEY ABBREVIATIONS

AI	Artificial Intelligence
GEOINT	Geospatial Intelligence
HUMINT	Human Intelligence
IMINT	Image Intelligence
NATJOINTS	Joint Operational and Intelligence Structure
NCC	National Communication Centre
NEC	National Intelligence Estimate
NICOC	National Intelligence Coordinating Committee
NSC	National Security Council
RICA	Regulation of Interception of Communications and Provision of Communications-related Information Act
OSINT	Open Source Intelligence
SAHRC	South African Human Rights Commission
SANDF	South African Defence Force
SAPS	South African Police Service
SIGINT	Signal Intelligence
SOCMINT	Social Media Intelligence Agency
SSA	State Security Agency
TOE	Technology Organisation Environment
UTAUT	Unified Theory of Acceptance and Use of Technology

CHAPTER 1: INTRODUCTION

1. INTRODUCTION

Technology is rapidly developing and will continue to impact our lives. Technology is used by the private sector to address a variety of issues that arise both domestically and globally. Among these challenges are cyberattacks, social media propaganda and other criminal activities. These challenges are not unique to the private sector as they are also experienced by the government and the intelligence communities. It is important for intelligence communities to undergoing the harsh emerging threats that come with technological advancements.

Social media is one of the platforms that present s numerous threats and it is described by Omand et al. (2012), as a "disruptive" phenomenon that has greatly aided in the explosion of information in the public domain. Both Facebook and Twitter (now known as X) were crucial in assisting the planning of rebellious activities and unrests in several Middle Eastern nations.

The disruptive nature of social media necessitated a response from government agencies to carry out various security tasks to manage the problem. Intelligence communities had to employ similar tactics, and they too had to use social media to enhance their investigation capabilities (Aldrich & Moran, 2019). Social media serves as a platform that allows intelligence agencies to collect and analyse data through various methods and at an accelerated pace in a world increasingly utilising 4IR technologies. Intelligence agencies are now gradually moving towards utilising social media for intelligence gathering. One of the intelligence collection disciplines that have been proven to be successful in countering threats to national security is social media intelligence (SOCMINT). In South Africa, social media is a new discipline in the intelligence field, and the country has been slow in recognising the value of SOCMINT as an intelligence discipline (Stegen, 2019). The slowness of the discipline adoption could have led to one of South Africa's intelligence failures in history (July 2021unrest).

Thus, the purpose of this study is to explore and explain the South African intelligence community's inability to anticipate the outbreak of the July 2021 civil unrest by failing to adopt and utilise SOCMINT as a tool to mitigate national intelligence threats. For this study, the July 2021 unrest was used as a case study. The outcome or the results of the study can be applicable

or used to avoid similar intelligence failures in the future or avoid civil unrest that will potentially be mobilised through social media intelligence.

1.1 Background

Information has been considered a significant aspect of power and a critical asset of any institution (Fulmer & Ployhart, 2013). For many organisations, the ability to handle information generation, management, and utilisation has emerged as a desirable power (Fulmer & Ployhart, 2013). Through advanced technology and the emergence of the internet and social media, the platforms have provided technological platforms for information gathering. Technology has been a factor of change, and the emergence of the 4th Industrial Revolution (4IR) has proven to have given government institutions, businesses, and intelligence communities new opportunities to gather, process, and interpret information (Toews, 2022). Over the last few decades, the internet landscape has become complex, characterised by ethnic groups within states, terrorism, criminals, extremist groups, cyber-attacks, and unrest mobilisation (Ganesh & Bright, 2020). According to Interpol, about 90% of terrorists' online operations are conducted through social media platforms, which are used for recruiting, funding, planning, and conducting terrorist attacks (Interpol, 2021). According to a study by Hamm & Spaaij (2015), up to 76% of post-9/11 lone wolf terrorists in the US announced their intentions using emails, texts, and, more significantly, Facebook posts and Twitter feeds. Putter & Henrico (2022), states that by 1999, most known terrorist organisations (Islamic State of Iraq and Syria, Al-Shabaab, and Al-Qaeda) were represented online. By 2000, most terrorist and extremist organisations had finished their transition from text-heavy websites to interactive forums (Momi, 2021). In response to technological advancement, in the late 2000s, the use of interactive forums by many groups had started to decline or stagnate, and popular social media platforms like Facebook and Twitter started to become notable channels for propagandising, recruiting, and sharing information within the various Islamist extremist communities (Putter & Henrico, 2022).

The technological advancements have redefined the role of humans in the intelligence collection process and necessitated a response from intelligence communities due to their impact on national security (Katz, 2020; Putter & Henrico, 2022). National security is a multidisciplinary matter and national interests such as technological security, infrastructure security, internal security, and economic security are only a few examples of the diverse core

values that make up the multidisciplinary field of national security (Dover, 2020). In the context of this study, any activity that compromises internal stability, and affects political stability, economic stability, social stability, and societal peace can pose a threat to national security. Therefore, it is necessary to understand the purpose and functions of the intelligence community because they must alert and forewarn the Government of any threats to national security, with the Government having the ultimate responsibility for taking action (Dover, 2020).

Already in 2014, the activities of extremist groups on social media had decreased over the years (McLoughlin et al., 2020). As the policing of established forums has increased, public confidence has declined, which has contributed to the relative reduction in the relevance of internet forums within some extremist organisations, which also matches the decline in the use of internet forums generally (McLoughlin et al., 2020). Due to the popularity of social media websites, organisations now use the platform to plan and organise events for protests and large-scale public demonstrations (Khan, 2022). Since the dawn of Democracy, South Africa is now characterised by the proliferation of public protests which pose a threat to national security (Vhumbunu, 2021). Civil unrest research suggests that most protests today are organised and planned well in advance (Sech et al., 2020; Vhumbunu, 2021). This is because the social media landscape has evolved over the years due to the digital revolution and its application in the world without boundaries. The use of social media has evolved, and it is now able to function as a real-time intelligence system thanks to the quick updates provided by social networks. Intelligence analysts can gather information about ongoing events in real time whether they are routine or crisis events. As a result, political, socioeconomic, and national security dynamics are being dramatically influenced by social media to the point that instability is being promoted (Jain & Vaidya, 2020).

Maniscalco (2012), states that to comprehend a country or even a community, one needs to have an in-depth and thorough understanding of its online or virtual community. As more people post information about their lives online, they therefore become of interest to businesses and government institutions. One of the biggest variables in the field of technology has been the development, establishment, and growth of the Internet. DataReportal (2023), estimated that by January 2023, there were 5.44 billion internet users worldwide (about 68% of the world's population), with 43.48 million of them in South Africa. South Africa was home to 25.80 million social media users in January 2023, equating to 42.9 percent of the total

population (DataReportal, 2023). The consequence of the internet development was the phenomenon of social media, which has greatly aided in the explosion of information in the public domain or, as it is often known, big data (Senekal, 2018). The reality that criminals like drug traffickers, human traffickers, and terrorists use social media to further their illegal ends is still a fact (Putter & Henrico, 2022). This necessitates a response from government agencies to carry out various security tasks to manage the problem. Intelligence communities had to employ similar tactics, and they too had to use social media to enhance their investigation capabilities (Aldrich & Moran, 2019).

Social media is one of the platforms that has made it possible for intelligence communities to gather and analyse information through multiple means and at a faster rate in a world where 4IR technologies are becoming more widely used. Intelligence communities are now gradually gravitating towards the use of social media as a form of intelligence collection, especially with the rise in popularity of the internet since the early 2000s (Marcellino et al., 2017). Over time, the use of social media as a platform for intelligence gathering has increased quickly (McLoughlin et al., 2020). Omand et al. (2012), were inspired by this use of social media and they referred to this phenomenon as a "disruptive technological development", making the platform relevant to security and public safety because criminals use cyber security to achieve their criminal objectives and terrorist groups use the social media platform to distribute their ideology, recruitment campaigns and propaganda (Interpol, 2021). For example, in 2019 Ghanaians were recruited by ISIS through social media propaganda and violent extremist groups operated by Burkina Faso. According to Vhumbunu (2021), about 100 Ghanaians were recruited through social media by ISIS and they joined the organisation in Libya (Kofi Aubyn, 2021). Thus, countering threats to national security can be done more successfully by investing in social media intelligence (SOCMINT).

1.2 Contextualisation

Literature by Omand, Bartlett and Miller (2012); Ronn and Soe (2019), define SOCMINT as data obtained from social media sites and the technologies used to analyse it. Ivan et al. (2015); Davis (2015); Norton-Taylor (2015), concur with the definition suggesting that it is the process of identifying, collecting, validating, and analysing data from social media platforms and accounts using non-intrusive and/or intrusive techniques to produce intelligence that reduces the level of uncertainty in decision-making and/or to develop products for national security.

The emphasis of both definitions is on comprehending, analysing, and predicting behaviours, disasters, and occurrences. Given that the intelligence organisation's mandate is to alert or fore-warn the government about an impending security threat and mostly rely on covert operations to exclude their mandate. The South African civil intelligence's mandate, according to the State Security Agency (SSA) website 2023, "is to provide the government with intelligence on potential threats to national stability, constitutional order, and the security and well-being of our citizens from both domestic and foreign sources". This applies to both the South African Defence Force (SADF) and the South African Police Services (SAPS). The mandate for military intelligence functions is the same as for civilian intelligence functions while the SAPS utilises social media for criminal activities. Thus, the intelligence services must continuously consider how to stay relevant to the political climate and in the current digital world. With both definitions in mind and an understanding of all intelligence organisation's mandates, SOCMINT should be incorporated into the intelligence framework, as its ineffective use has resulted in numerous intelligence failures (Wankhade et al., 2022), including the July 2021 civil unrest, the Arab Spring, and the 2011 London riots, among others. These incidents have shown how social media can gather information in real-time to help prioritise and facilitate activities that need to be taken to resolve crises. Stegen (2019), states that traditional intelligence indicators may have been irrelevant given that the Arab Spring and 2011 London uprisings and unrests were organised online. The July 2021 civil unrest report concurred with Vhumbunu (2021), thinking that the July 2021 uprising was also organised online. Forrester et al. (2016) and Momi (2021), describe social media as a powerful potent force in and of itself, due to its capacity for information dissemination, making it extremely "irrepressible". Thus, if SOCMINT is not adopted as an intelligence collection discipline by government agencies, those individuals or organisations looking to engage in harmful activities will increasingly use social media as their preferred unrestricted and unmonitored communication channel (Ivan, 2015; Dover, 2020).

Omand et al. 2012; Montagnese (2012) and Dover (2020), present SOCMINT opportunities that can mitigate threats to national security, however in literature, there is some debate that while SOCMINT contributes to situational awareness following an incident (Dover, 2020), it is unable to foresee immediate threats and lay a solid groundwork for intelligence production (McLoughlin et al., 2020). As a new intelligence collection discipline, SOCMINT poses some challenges to those seeking to exploit it. Some of these challenges include validation and technology challenges (Momi, 2021). In addition, the biggest SOCMINT issue arises when

someone intrudes into another person's personal space or when an intelligence agent uses invasive techniques to gather information of concern to national security (Omand et al., 2012). The intelligence community's adversaries like Al-Shabaab are highly active on social media for their agenda and mandate, thus making SOCMINT a two-edged sword (Momi, 2021). Thus, it is important to develop a legislative framework that will mandate and guide the use of SOCMINT inside the intelligence environment. Unfortunately, in South Africa, there is currently no legislation that governs the use of SOCMINT as an intelligence collection discipline (Putter & Henrico, 2022). In South Africa, social media is a new discipline in the intelligence field, and the country has been slow in recognising the value of SOCMINT as an intelligence discipline (Stegen, 2019). The slowness in gravitating towards the use of SOCMINT as an intelligence discipline could have led to one of South Africa's intelligence failures in history due to a lack of response by the intelligence and law enforcement institutions in the July 2021 civil unrest following the arrest of the former president of South Africa Jacob Zuma.

There are no apparent studies that have examined the use of SOCMINT as a tool for mitigating national security threats in the African context. Therefore, this study will fill that gap in the literature. The theoretical framework for this study originates from the social sciences. The Unified Theory of Acceptance and Use of Technology (UTAUT) and Technology Organisation-Environment (TOE) framework apply to Social Media Intelligence studies, the latter being the main adopted theory for this study. This will be discussed further in Section 2.12.

1.3 Problem statement

The internet is used by terrorists or radical groups to spread propaganda, recruit new members, communicate, collect intelligence, look for funding, and even inspire and plan attacks. According to Bartlett and Reynolds (2015), by 1999, the majority of terrorist organisations were represented online. For example, 90% of data needed by the CIA Bin Laden unit came from open-source intelligence (Gompert et al., 2003). In contrast, the former Deputy Director of the CIA argued that 95 to 98% of the information provided by the American intelligence agencies came from open source (Gompert et al., 2003). Popular social media sites like Facebook and Twitter began to emerge as significant routes for information exchange within the various Islamist extremist communities in the late 2000s (Bartlett & Reynolds, 2015; McLoughlin, 2020). The September 11, 2001, terrorist attack became the main danger to the

world's security, therefore, most governments responded to the event by developing new legislation framework to enhance "international" and "regional" security, the majority have created international agreements with allies and developed countries like Britain and United States (US) initiated several national security technology adoption programs to improve how intelligence is gathered and analysed (Whelan, 2012). The opportunities for using social media as an intelligence collection discipline are so extensive that the National Guard in Russia is training Russian Army specialists in SOCMINT operations (Golts, 2017).

However, in South Africa, social media is a new discipline for intelligence gathering and the country has been slow in recognising the value of SOCMINT as an intelligence collection discipline (Stegen, 2019). The slow recognising or adoption of SOCMINT as an intelligence collection discipline led to one of the country's intelligence failures since the dawn of democracy. In July 2021, violent civil unrest broke out in Gauteng and parts of KwaZulu Natal. Social media mobilisation during the upheaval led to looting and economic damage, among other things (Civil unrest report, 2021). The expert panel's study of the civil unrest in July 2021 suggests that social media and open-source software were mostly responsible for the carnage (Civil unrest report, 2021). Thus, traditional intelligence collection disciplines like human intelligence (HUMINT) were irrelevant. According to the civil unrest report (2021), security services appeared perplexed using social media and open-source platforms, which prevented them from processing the information spreading in communities and from putting operational plans in place to address the national threat. The South African intelligence community is still struggling or has not adapted to the new technology landscape (SOCMINT), therefore rendering them irrelevant (Stegen, 2022; Putter & Henrico, 2022).

There is growing interest in social media intelligence research in the intelligence community globally. However, most research study on intelligence includes a wide range of topics that aid in comprehending the role of SOCMINT and its significance to national security (Antonius & Rich, 2013; Dover, 2020; Ivan 2015; Momi, 2021; Thapa, 2020). The literature is crowded with studies that focus on the application of SOCMINT to identify terrorism threats, opportunities, and challenges of SOCMINT and there is little research on the utilisation of SOCMINT for predicting and identifying online civil unrest. Those who have researched SOCMINT to mitigate civil unrest or radicalisation threats (Agarwal, 2015; Bartlett and Miller, 2015; Stegen, 2019) were based on a systematic review approach. Most previous work has been conducted in developed nations, and little attention has been paid to developing nations

such as South Africa. There is a limited research study that focused on the state of SOCMINT adoption and use to mitigate national security threats in South Africa where primary data was collected.

With organisations across different intelligence communities in South Africa having understood the value of social media and opportunities presented by technologies such as SOCMINT, questions arise as to why its adoption and use in the South African intelligence community remains relatively low, and what challenges are presented by SOCMINT. Thus, the purpose of this study was to gain insight into the challenges of adopting SOCMINT in the intelligence community in South Africa. This is further broken down into research questions and objectives as discussed in the next section.

1.4 Research questions

The main research questions for this study is:

Why is the adoption of SOCMINT in the South African intelligence community relatively low, and what challenges are presented by SOCMINT? (Specific focus on the July 2021 unrest).

The following sub-research questions will help in answering the main research question:

1.4.1 What are the primary obstacles to recognising SOCMINT as an official intelligence collection discipline within the intelligence community?

1.4.2 What factors impede the effective adoption of SOCMINT, and what challenges are encountered during its execution?

1.4.3 What extent of information was accessible to the intelligence services to adequately detect, comprehend, and respond to both the threat and the actual outbreak of the July 2021 unrest violence?

1.5 Research Objectives

1.5.1 To investigate the primary obstacles to recognising SOCMINT as an official intelligence collection discipline within the intelligence community.

1.5.2 To investigate the factors that impede the effective adoption of SOCMINT, and what challenges are encountered during its execution.

1.5.3 To investigate if the intelligence services had access to a significant amount of information to effectively detect, comprehend, and respond to both the threat and the actual outbreak of the July 2021 unrest violence.

1.6 Purpose of the study

This research investigates the concept of SOCMINT and its impact on national security threats. The study explains the South African intelligence community's failure to recognise SOCMINT as an intelligence collection discipline as a result of failing to anticipate the July 2021 civil unrest. Many research studies have proven that SOCMINT can provide accurate warning indicators to intelligence agencies where traditional intelligence collection disciplines are too risky or difficult to use (Bartlett & Reynolds, 2016; Stegen, 2019).

This study gained understanding and insights into the challenges of adopting and utilising SOCMINT as a tool to mitigate threats to national security. The study also attempted to identify factors or vulnerabilities that have hindered the utilisation of SOCMINT by South African intelligence organisations, reasons for the existence of the challenges or vulnerabilities, and viable solutions are also provided through this study.

1.7 Research limitations

The United States, the United Kingdom (UK), Israel, and Australia are frequently represented in the literature on intelligence failures. Considering the 195 countries of spy services around the world, this sum is unquestionably insignificant. There is a conventional view that everything related to intelligence collection should be kept a secret, especially in developing countries due to limited research studies on intelligence (Genidy, 2018). The sensitive nature of the environment could be a reason there is resistance to sharing information.

One of the limitations of this study is the inability to use classified information. Credible classified information about the use of SOCMINT for intelligence and security information collecting does exist, but it is not accessible to the public due to the "need-to-know" principle and a lack of security clearance requirements. Given the goal of investigating and discovering the facts related to understanding a phenomenon in a real-world intelligence community setting, the restrictions were not significant, because the President of the Republic of South Africa announced a panel to explore and review the country's readiness and inadequacies response to the unrest. Thus, critical individuals (from different intelligence structures) who

were deemed integral to the study were interviewed and questioned on the role they played in providing sufficient warning indicators before the unrest. Additionally, SOCMINT as a field of study and a discipline of intelligence naturally focuses on the analysis of information that is public or semi-public.

A certain intelligence organisation did not allow for one-on-one interviews due to the sensitivity of the environment. Instead, participants who knew the organisation was interviewed to get their perspective on the adoption of SOCMINT in that particular organisation.

The second limitation was concerning accessibility to participants. The sample was restricted to intelligence officials from two intelligence organisations and retired intelligence experts who know of intelligence gathering, with a specific focus on intelligence agencies. The researcher intended to gather data from all three intelligence communities (Defence, SSA and SAPS), but due to the sensitively of the environment, two communities were willing and gave consent to data collection. This limitation did not restrict the information gathered because two of the identified participants had knowledge and expertise of all the intelligence communities. Thus, the three different intelligence perspectives were established.

1.8 Intended contribution

The technological capabilities are improving the intelligence community in a world of greater threat and greater transparency; thus, intelligence communities can maintain information advantage through the intelligence collection disciplines. However, terrorist organisations are using the same disciplines to recruit, plan an event, communicate their ideology, therefore creating a threat to national security (Hamm & Spaaij, 2015; Jain & Vaidya, 2020). Unrest was also becoming characterised by social media mobilisation leading to violence, damage to property and threating national security. Thus, countries like South Africa are likely to experience outbursts of riots and unrest and intelligence failures are inevitable as history has shown.

Research studies of intelligence include a wide range of topics that aid in comprehending the role of intelligence and its significance to national security. Literature is crowded with case studies and the study of intelligence failure, however, there are limited studies that explain the challenges or vulnerabilities of adopting and utilising SOCMINT within the South African

perspective. Moreover, South African research studies of SOCMINT are strictly restricted from secondary sources. However, this study explored the intelligence community's perspective and views of their experience and use of SOCMINT as an intelligence collection discipline and their challenges in utilising SOCMINT as a tool of mitigating national security.

Given the problems and the cleavages in South Africa's society, it is unlikely that the country will not experience outbursts of riots and looting. Since South Africa has experienced economic and social unrest ever since the country transitioned to democracy in 1994 (Smith, 2021; Musumeci, 2021), this study provides recommendations on systems that need to be put in place to forewarn and eventually respond to unrest or similar occurrences that may pose a threat to national security. The impact of varied contextual conditions on SOCMINT adoption can be explained by looking into various intelligence structures within the intelligence community and their diverse mandates. This study highlights key factors that the intelligence community may consider in setting a supportive regulatory environment. The findings of this study also assisted with theory building research to better explain how the interrelated challenges work together to prevent SOCMINT adoption.

1.9 Research Methodology Approach

The study aimed to investigate the South African intelligence community's challenges and vulnerabilities in adopting SOCMINT as a tool for mitigating national intelligence threats as a result of failing to predict or prevent the July 2021 unrest. The research methodology adopted from Saunders, Lewis and Thornhill (2009), and it followed the following layers:

1.9.1 Philosophical: focus on what we know about the world and how we got to know about it. An interpretive paradigm was selected for this study.

1.9.2 Research Approach: Saunders et al. (2009) identify two research approaches, inductive and deductive. In this study, inductive is an adopted approach for this study because this research looked to understand the perceptions and behaviour of individuals in the intelligence community.

1.9.3 Research Design and Strategy: A qualitative research approach expresses interpretive data whereby, findings are produced through observation and interviews to obtain logical interpretation and conclusions (Hammarberg, Kirkman and de Lacey, 2016).

The qualitative approach was used to provide a holistic viewpoint of the research. An exploratory research design was chosen using a case study because exploratory research is conducted when a problem is present but not well characterised (Du Plooy-Cilliers et al., 2014). A case study through the interpretive paradigm provides a comprehensive and concentrated understanding of a case under study. In this situation, the research's objective was to explore and investigate the South African intelligence community's challenges and vulnerabilities in utilising SOCMINT as a tool to mitigate national intelligence threats as a result failing to predict or prevent the July 2021 unrest.

1.9.4 Time horizon: This includes longitudinal time horizon and cross-sectional time horizon. Longitudinal time horizon focuses on observing a group over a period and cross-sectional studies of a phenomenon at a particular time. This study focused on a cross-sectional approach.

1.9.5 Data Collection and Analysis: The last layer of the research onion addresses the data collection method and the data analysis technique. This refers to the collection activity of the information and the process of bringing order, structure, and meaning to the data. Data was collected through interviews and a thematic analysis technique was selected for this study.

1.9.6 Sampling: A sampling strategy was based on the non-random selection of Intelligence Community (IC) experts and analysts. The focus of the study concentrated on individuals and experts who have knowledge of social media from the perspective of national security threats and intelligence specialists who have used SOCMINT for intelligence gathering.

1.9.7 Theoretical Framework: The study aimed to investigate the South African intelligence community's challenges and vulnerabilities in adopting SOCMINT as a tool for mitigating national intelligence threats as a result of failing to predict or prevent the July 2021 unrest. Thus, the TOE theory together with UTAUT is adopted to study the factors that influence the adoption of technology. It is important to determine the likelihood of SOCMINT adoption by the South African intelligence community.

1.10 Summary

The use of SOCMINT has created a wide range of opportunities for both public organisations and intelligence services (including those involved in terrorist or criminal activity). Incorporating SOCMINT techniques as an intelligence collection discipline enhances protection against terrorism threats or any civil unrest activities that pose a threat to national security. Government and peoples' perceptions of intelligence, according to Michael Herman, will be forever impacted by the events of September 11th (Herman, 2009). In the South African context, the perceptions of intelligence will be affected and remembered by the July 2021 civil unrest. The significance of social media intelligence as a discipline for gathering intelligence has been established in the literature, but the diagnostic, legal, and regulatory systems have not kept up with the globalisation that technological innovation has made possible. This necessitates actions to channel knowledge, innovation methods, and contributions of individuals or organisations throughout the world, to seriously pursue the trend toward real-time data. The intelligence organisations in South Africa need to institutionalise and operationalise SOCMINT in the intelligence framework. The study aimed to explore and gain an understanding and insight into the challenges of adopting SOCMINT as a tool for mitigating threats to national security.

CHAPTER 2: LITERATURE REVIEW

2. INTRODUCTION

According to Toffler (2022), the three facets of power are wealth, violence, and knowledge, with the latter being the most crucial due to its effectiveness and adaptability. Additionally, he asserts that "knowledge is the most democratic source of power" (Toffler, 2022). Today's borderless world is overflowing with information, making it crucial to identify reliable sources of knowledge. Therefore, the literature review's primary objective is to provide a thorough grasp of South Africa's slowness in recognising the value of SOCMINT as an intelligence collection discipline, because the slow recognising or adoption of SOCMINT eventually led to the July 2021 civil unrest. The in-depth knowledge of the identified problem was explored through several journals, books, relevant documentation, internet articles, South African legislature, and PhD thesis. This chapter will explain the key concepts such as Intelligence, SOCMINT, and social media. In addition, it will discuss the role of intelligence and its application to national security, the effectiveness of SOCMINT as an intelligence collection discipline, and the social media landscape and its impact on national security. Moreover, the study discusses why countries failed to detect threats of national security. Furthermore, the study provide SOCMINT opportunities and challenges. The international legal, ethical, and privacy considerations are discussed versus the SOCMINT regulations in South Africa. Lastly, the chapter also considered literature on the theoretical framework of SOCMINT.

2.1 The role of intelligence and its application to national security

Understanding the purpose and function of intelligence is crucial before we can contextualise the role of intelligence in national security. The primary function of intelligence has remained consistent throughout history. The primary goal of intelligence is to assist in the formulation of policy (O'Connell, 2005). It is appropriate to add national security to this description. Thus, the goal of intelligence is to assist in the formulation of policy to maintain national security (O'Connell, 2005). Lowenthal (2022), asserts that policymakers can only make sound decisions if they are well-informed about both internal and foreign security issues. The intelligence community provides this information according to government priorities. In the instance of South Africa, national intelligence priorities are developed by the National Intelligence Estimate (NIE). The intelligence community must alert and forewarn the government to any threats of national security, with the government having the ultimate responsibility for taking upon action. National security being defined as people of the nation

living in peace and harmony, in a secure safe space with no fear and free from threat (South African Constitution,1996).

Within the South African context, the intelligence capacity existed since 1910, when the modern South Africa state was founded (O' Brien, 2010). The post-apartheid intelligence has since evolved, and the intelligence approach focus has also changed. During the apartheid era, the focus was on liberation movements but in the post-apartheid era, there was a wider range of appreciation of risks and threats that would impact national security (Stegen, 2020; Putter & Henrico, 2022). This is because South Africa is now characterised by the proliferation of public protests which pose a threat to national security due to political and economic changes (Stegen, 2019 & Vhumbunu, 2021).

Technology is also confronting the changes in the intelligence community because of its impact in national security. According to Mostert (2017), technology evolved from the use of radios and telephones for interceptions by the apartheid government. Currently, emerging technology like artificial intelligence (AI), cloud computing, social media, big data analytics can enhance and automate the intelligence collection disciplines (Katz, 2020). For example, with the aid of AI, analysts should be able to sort through social media platforms to find patterns, trends, and threats, visualise them, and then incorporate them into their analyses (Hershkovitz, 2019). To disseminate critical information and guide decision-making, cloud and AI solutions can help transform how intelligence is shared and provided more broadly amongst analysts, government, and intelligence agencies (Yu, 2023). Big data text analytics techniques on the other hand are used to mine and adopt opinions from the internet and real time social media data. However, technological skills deficit in South Africa will make it difficult to absorb the investigation methods because according to the World Economic Forum (2020), learners in South Africa reach matric without ever interacting with a computer and developing countries are characterised by limited knowledge, understanding and expertise in technology contrary to developed countries (Barros & Lazarek, 2018).

According to Lowenthal (2019) and Sauerwein (2021), the functions of intelligence include: predict, warn and inform. It is important for intelligence organisation to provide early warning to government of threats to and opportunities for national security. With the understanding of the functions of intelligence, the researcher hopes to determine if the South African intelligence services had the capacity, expertise, skill and knowledge to predict, warn and inform

government of the July unrest. According to the civil unrest report (2021), evidence was received on the effectiveness of the intelligence communities in forewarning and predicting the unrest and violence never before seen in democratic South Africa. Most members of civil society, as well as the provincial and national administrations, believe that the July occurrences were a serious intelligence failure (Civil unrest report, 2021). On the other hand, the intelligence community believe that it provided adequate warning, at least on the levels of public discontent amongst the population and the risks and potential consequences thereof. According to a report by the expert panel (Civil unrest report, 2021), the unrest was characterised by social media mobilisation leading to violence, damage to property, looting and disruption to economic activities and intelligence services were unable to foresee the type, scope, and tactics of the violence. Instigators shared posts, feeds, photos, blogs, files, photos, and more, about the planned event because these social networked outlets offer real-time, first-hand information (Civil unrest report, 2021). The intelligence services failure to predict the scale, nature and modus operandi of the instigators could be because of intelligence failure to use its powers. The civil unrest report (2021) concurs with this fact indicating that the intelligence services are in possession of the most invasive state capabilities, but they did not make full use of these powers in time and before the outbreak of the violence.

With the evidence provided by the civil unrest report (2021), the need to re-establish a reliable and capable intelligence service is even more urgent by the prospect that the unknown individuals who conducted this attack on the state were aware of its security agencies' flaws. According to Marais (2018), it is alleged that the civilian intelligence agency State Security Agency (SSA) was repurposed by the Former President Jacob Zuma to help him maintain his grip on power. The high-level review panel established in 2018 emphasised that during Former President Jacob Zuma's tenure (May 2009 to February 2018) SSA was one of the many institutions that were repurposed for illicit personal or political advantage (Marais, 2018). The importance of re-stablishing a reliable and capable intelligence service was emphasised by the then Minister of State Security, Dipuo Letsatsi-Duba, in her budget speech (SSA Budget Speech, 2018). According to the Minister, the SSA's governance and operational shortcomings must be urgently investigated (SSA Budget Speech, 2018). The agency has been in a constant state of transformation, which has led to fundamental structural and governance flaws (SSA Budget Speech, 2018). As a result of the situation in the SSA, President Ramaphosa was compelled to convene a high-level review panel in June 2018 (Mahlase, 2018). The panel's chair was the former Minister of the Police, Sydney Mufamadi. The panel was meant to identify

all relevant causes that contributed to some of the agency's current issues and challenges so that necessary steps can be taken to prevent a repeat of state capture (Mahlase, 2018).

Intelligence has different meanings to different people and the South African civil intelligence seems to have miss-defined the institutional purpose and mandate but Kent brings meaning and purpose to the definition. The majority of the definitions of intelligence are based on Kent's (1966) characterisation of the idea as "the knowledge which our highly positioned civilian and military officers must have to defend the national welfare". In addition, Kent (1966), emphasises that when intelligence professionals use the term intelligence, three qualities are meant. The three dimensions are, prescriptive, anticipatory, or descriptive intelligence (Clarke, 2010). The intelligence can either recommend a course of action for decision makers, predict possible futures, describe what happened or what is happening. The intelligence definition defines the intelligence process as demonstrated in Figure 1 below.

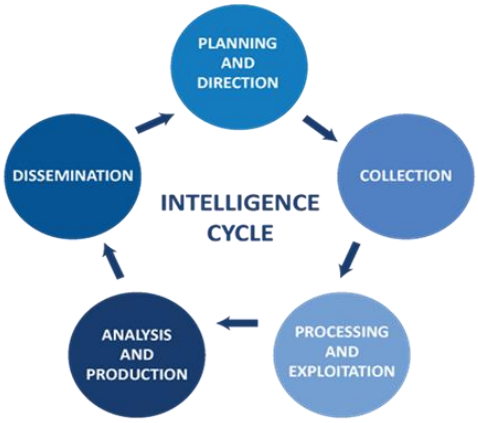


Figure 1. Intelligence Process (Lowenthal, 2022)

The traditional intelligence tradecraft includes collection, analysis, covert operations, and counterintelligence (O'Connell, 2005). Jones (2007) defines collection as gathering information about an event, a group, individuals, and activities that are of national threat or interest. Particularly focusing on terrorism, organised crimes, espionage, and sabotage. Analysis is a term used for transforming raw information into intelligence through the process of collecting, analysis, and evaluating data (DCAF, 2003). Erwim (2013), defines covert operations as an attempt to "elicit change in the political, economic, military, or diplomatic behaviour of a target". Counterintelligence function involves protecting the country, as well as intelligence agencies, from the activities of foreign intelligence service (O'Connell, 2005).

Information collected through the traditional intelligence tradecraft is considered intelligent if it is relevant, timely and accurate for decision making (O'Connell, 2005).

2.1.1 Five Main Intelligence Disciplines

Omand (2017), argues that information must meet certain criteria in terms of how it is obtained, supported by evidence, confirmed by other sources, comprehended, and used before it can be termed successful "intelligence." To achieve this, common forms of intelligence collection disciplines have been used over the years within the intelligence community, and they are currently recognised as the five main intelligence collection disciplines (Lowenthal & Clark, 2015) as discussed below:

2.1.1.1 Signal Intelligence (SIGINT), intelligence technology to intercept satellite communication (Ball, 1989). In today's definition, it is defined as intelligence that is derived from electronic data and communication using Artificial Intelligence (Bernard et al., 2020). The SIGINT technological efforts have improved over the years, but the definitions are similar because they incorporate the key fundamental principles of SIGINT, communication intelligence and electronic intelligence (Weinbaum, 2017 & Richelson, 2018). Communication intelligence is information derived because of intercepting communication from e-mails, phone calls or messages and other communication systems (Richelson, 2018). Electronic intelligence does not contain interpersonal communication because it intercepts radar signals (Kaminski, 2019). The use of SIGINT date back to the first world war when the British Royal Navy began to intercept the German's radio communication to monitor their plans (Ball, 1989; Aid & Wiebe, 2010). As technology has evolved, so has the SIGINT capabilities. Today, the US intelligence communities collect intelligence through drones, Unmanned Ariel vehicle, satellites, advanced sensors, cyber collection (Clark, 2020). This technology enables greater penetration of denied areas and it can assist analysts in how they receive data to study patterns, trends and develop warning indicators for decision makers.

2.1.1.2 Open-Source Intelligence (OSINT), dates to the emergence of intelligence as a supporting tool to government decisions (Schaurer & Jorger, 2010). Before the arrival of the internet, OSINT was defined as unclassified information derived from publicly accessible and openly available sources, such as newspapers, books, conference, and journal (Shulsky & Schmitt, 2002). The use of open source has rapidly increased over

the years, especially in the popularity that the internet has gained since the early 2000s. The definition changed after the introduction of the Internet and it now includes computer-based information (Williams & Blum, 2018). The introduction and application were because of conflict, threats and potential attacks from terrorism and cyber espionage (Senekal & Kotzé, 2019).

2.1.1.3 Human Intelligence (HUMINT), Human intelligence is the oldest of intelligence collection disciplines until the revolution of technology. According to Kent (1964); O'Cornell (2005); Crosston & Valli (2017), HUMINT remains the important and the primary method of intelligence collection because technology cannot provide human emotions and perspective. Moffet (2021), states that technical intelligence collection disciplines are limited to determining human intention capabilities and human collectors can provide insight into the human perspective. Hulnick (2006), defines HUMINT as collecting information covertly (sensitive classified information), overtly (can include published materials etc.) or through clandestine operations (recruited agents or volunteers who are willing to provide information to foreign nations). It is an adaptable method for rapidly collecting, processing, analysing and acting on collected information for decision makers (Kent, 1964). Obtaining information from human sources is primary the domain of intelligence agencies (Kamiński, 2019). One can image that collecting information from humans is time-consuming than using technological intelligence sources. The use of human intelligence, especially covert agents, necessitates extreme caution and carries a significant risk, for example individuals who are revealed by counterintelligence services may be charged with espionage. Additionally, some human intelligence sources may end up being "double agents" who covertly work for another intelligence service.

2.1.1.4 The Geospatial Intelligence include "perception, cognition, computation, control, reaction, and understanding of physical features with geographically referenced activities" (Bacastow & Bellafiore, 2009). According to Margolis (2013), GEOINT as an intelligence discipline involved "coordinating the collection by various capabilities of intelligence communities (aircraft, satellites and Unmanned Arial Vehicles), processing and analysing these images and disseminating the results". The use of Unmanned Arial Vehicles by the US intelligence was considered the most significant innovation because of its ability to provide broad overview and systematic surveillance

using high-resolution synthesis (Margolis, 2013). The technology was able to deliver countless images, and it can get closer to the target without being detected. The Oboma administration relied on UAVs to penetrate closed societies (Crosston & Valli, 2017).

2.1.1.5 Image Intelligence (IMINT), Imagery intelligence is derived from the interpretation or analysis of images and other materials, and it includes technical, geographic, and intelligence information (Kamiński, 2019).

Any government's primary duty is to ensure the safety of its people, and if it does not fulfil this duty, it will be under tremendous public pressure. Technology development has changed how information is shared among people. Most governments find it difficult to monitor intelligence using solely conventional techniques in the tech-savvy era. For governments to effectively address current security concerns, the usage of SOCMINT is crucial.

By nature, SOCMINT could collectively capture a combination of the above-mentioned intelligence collection disciplines; a single entry could have an image, geographical information, and textual intelligence (Mahood, 2015). It is the youngest of the intelligence collection disciplines, though it is still earning it validity amongst the intelligence communities, the future of its ability in yet to prove itself in South Africa. However, SOCMINT has proven its effectiveness and ability in countries like United States and United Kingdom have recognised SOCMINT as an intelligence collection discipline (Hershkovitz, 2019).

2.2 Sub-categories of Intelligence Communities

According to the National Strategic Intelligence Act 39 of 1994, the purpose of intelligence services and agencies is to gather and analyse "intelligence" to enable responses to threats (potential or identified) to the security of the Republic or its citizens (Constitution of the Republic South Africa, 1994). Currently, the following intelligence communities exist in South Africa: State Security Agency (SSA), Crime Intelligence under South African Police Services (SAPS) and Defence Intelligence under South African Defence Force (SANDF). The South Africa civil intelligence organisation State Security Agency’s mandate refers to the delivery of preventative intelligence to the government of South Africa (Constitution of the Republic South Africa, 1994). The mandate for military intelligence functions is the same as for civilian intelligence functions; it focuses specifically on military operations with the same national goal. Domestic military intelligence is defined as "intelligence required for the planning and

conduct of military operations within the Republic to ensure security and stability for its people" (Constitution of the Republic South Africa, 2002). The investigation of social media in the use of criminal activities is the responsibility of the SAPS as set out in the 1996 Constitution of the Republic of South Africa. Each of these intelligence communities (military, criminal, and civilian) can use SOCMINT to mitigate national security threats.

The burning question is why the South African Government and security organisations were unable to foresee and stop the widespread violence of the July 2021 unrest despite having access to all the security resources the state could need and having systems in place for coordination at both the national and provincial levels. To facilitate operational and policy decision-making on security issues in South Africa, several coordination mechanisms have been put in place. These comprise of a National Security Council (NSC) at the top of the government, which is presided over by the President. Since 2000, the NSC has served as a crucial advisory body and contributed to the development of national security strategy (National Strategic Intelligence Act, 1994). The NSC oversees approving the National Intelligence Priorities, the National Intelligence Estimate, and the National Security Strategy. It also coordinates the efforts of the security services, law enforcement organisations, and other pertinent state organs to ensure national security and receives coordinated, integrated intelligence assessments from the national security structures (National Strategic Intelligence Act, 1994). The July civil unrest report raised concerns about overlapping of roles and lack of information sharing as the contributing factors to the intelligence failure (Civil unrest report, 2021).

For the successful implementation of SOCMINT as an intelligence collection discipline, these organisations cannot work in silos because the mandates of each organisation influence the facilitation of operations and policy decision making on security issues. The following sections presents the effectiveness of SOCMINT if it is adopted as an intelligence collection discipline.

2.3 The effectiveness of SOCMINT as an intelligence collection discipline

Social media data can be collected and used for a variety of purposes, and SOCMINT encompasses a wide range of methods, applications, and capabilities in doing so. Literature suggests that open-source intelligence (OSINT), is a subset of SOCMINT (Bartlett & Reynolds, 2013, Putter & Henrico, 2022). However, validity and interpretation must be taken into every specific account or consideration while using SOCMINT. The question of whether

SOCMINT belongs in the OSINT category or as a separate subcategory is currently up for discussion. How do SOCMINT and OSINT differ from one another? The distinction, by Putter & Henrico (2022), can be found in the content and sophisticated methods required to evaluate the relevance of the information. OSINT sources can be accessed without breaching any privacy laws (Ronn & Soe, 2019). Individual privacy settings limit access to unrestricted information on public social media platforms; for example, if a privacy option is set up in such a way, Facebook alerts sent by an individual are only visible to individuals in the individual's peer group. However, by definition, SOCMINT accesses all such data without taking privacy into account (Ronn & Soe, 2019; Putter & Henrico, 2022). The implications of concerns like the right to privacy then become apparent, indicating that SOCMINT is likely no longer included in the OSINT definition. However, when it comes to South Africa, the terms "transparency," "intelligence oversight," and "democracy," are important aspects to keep in mind when analysing the South African intelligence landscape (Putter & Henrico, 2022).

Intelligence organisations have always avoided accountability because of its secret nature of activities. Swart (2018), allegedly made claims that the South African government is using social media content to surveil its citizens, claiming that it is used against security threats. The July 2021, panel unrest concurred with Swart's (2018), claims, indicated that South Africa's intelligence agency is known for its controversial use of covert, intrusive and secret methods (Civil unrest report, 2021). SSA's controversial use of secret and intrusive methods were also highlighted in the 2018 Report of the High-Level Review Panel. It was found by the panel that SSA had been compromised by mismanagement, factionalism, and incompetency (Civil unrest report, 2021).

SOCMINT consists of intrusive social media collection and open-source collection. Omand et al. (2017), argued that security community must incorporate SOCMINT into the framework for national intelligence, but only after passing two crucial requirements. The first is that it is based on a strong methodological foundation of data gathering, evidence, verification, understanding, and application (Omand et al., 2017). The second is that the moral risk it presents can be justified. Many countries around the world are using SOCMINT to observe, watch, listen, understand, and ideally predict activities that may threaten national security (Putter & Henrico, 2022). The Boston Police Department utilised Twitter effectively during the Boston Marathon bombings to inform the public on the investigation's progress, to soothe tension and solicit support from the public, and to dispel fabricated media reports (Lumpp,

2014). To track down and recruit Palestinians to spy on Hamas, Israel used the personal information posted on Facebook (Kubovich, 2016). In Kenya, twitter played a crucial role in facilitating communication between emergency personnel, the government, and the public during the four-day terrorist siege of the Westgate Mall in 2013 (Davis at al., 2014). Kansas City No Violence Alliance employs social media intelligence in its model as part of an initiative to create a predictive instrument for potential offenders (Privacy International, 2017). Developed countries like United States (US) and Britain have leveraged the technical intelligence technology to improve how intelligence is gathered and analysed. The UK intelligence agency Government Communications Headquarters (GCHQ) created the Squeaky Dolphin program to gather and analyse data from social networks with the goal of tracking the nation's opinions toward politicians and sports (Kelion, 2014; Privacy International, 2017). In the US for example, companies like Cisco and Nec offer intelligence agencies a variety of analytics solutions such as identity analytics, social media analytics and video analytics (Hershkovitz, 2019). These platforms help government agencies use real time data stream analysis and machine learning to derive insights and make predictions from historical data collected (Hershkovitz, 2019). Although intelligence organisations are silent about the rationale behind this approach, it could be due to a lack of knowledge and skills within these organisations. This does not mean that SOCMINT is beginning to dislocate other intelligence collection discipline, rather it is beginning to catch attention because of how social media is used to threaten national security.

Human intelligence (HUMINT) is the oldest form of intelligence collection until the revolution of technology (Margolis, 2013; Kamiński, 2019; Stegen, 2019). According to Kent (1964); O'Cornell (2005); Crosston & Valli (2017), Kamiński (2019); Stegen (2019), HUMINT remains the important and the primary method of intelligence collection because technology cannot provide human emotions and perspective. Momi (2021), state that HUMINT is the only intelligence collection discipline that can read body language and human mind. Beauman (2013), state that technical intelligence collection disciplines are limited to determining human intention capabilities and human collectors can provide insight into the human perspective. Hulnick (2006), defines HUMINT as collecting information covertly (sensitive classified information), overtly (can include published materials etc.) or through clandestine operations (recruited agents or volunteers who are willing to provide information to foreign nations). It is an adaptable method for rapidly collecting, processing, analysing and acting on collected information for decision makers (Kent, 1964). The bias and the use of human information

technique is most common in developing countries and warfighting countries (Crosston & Valli, 2017, Katz, 2020). However, Putter & Henrico (2022), argues why risk human asset if similar information can be obtained through technological advancements.

The technological capabilities for intelligence collection have quickly drawn the attention of the intelligence services, particularly the Central Intelligence Agency (CIA), which has become infatuated with its capabilities (Margolis, 2013) the rationale behind the obsession is because it reduces human loss, and it is adaptable in various contexts. The reliance on technology created imbalance in the use of other collection discipline, which has had a negative impact on intelligence quality resulting in many intelligence failures (Nygaard, 2014). The inadequate use of HUMINT resulted in US's greatest intelligence failures, 9/11 attack and Iraq pre-was intelligence in 2003 (Margolis, 2013; Crosston & Valli, 2017). Thus, it is important to have mutual collaboration between human and technology collection method because human assets can never be fully eliminated no matter how technology evolves.

Although HUMINT remains a crucial core tradecraft for intelligence collection, emerging technology, particularly social media could transform the intelligence collection tradecraft. While personal interaction is crucial for agent handling and clandestine operations, agents today can be identified, assessed, developed, recruited and managed virtually (Katz, 2020). Thus, the blending of HUMINT and social media can enable more penetrating intelligence operations.

2.4 Social media landscape

Due to the digital revolution and its application in the world without boundaries, communication and exchange of thoughts can take place from anywhere in the world. Currently, information and ideas are freely transferred on the internet. More social interactions occur online, where rules and regulations are hard to implement because a single governing authority does not govern the area. As a result of its ungovernable nature, social media can never be seen as merely another forum for conversation, but as the "go-to" medium for influencing or shaping narratives across all spheres of state authority or power to protect the interests of nations (Putter & Henrico, 2022). Consequently, it serves as a key enabler of national intelligence. For this reason, Omand et al. (2012), describe social media as a "disruptive" phenomenon that requires a response from authorities.

Understanding human behaviour and how it affects national security is the core objective of intelligence (Lowenthal, 2022). Social interaction and communication are two of humanity's most basic requirements. The best way to fulfil that basic psychological is through social media. This widespread use of social media has given society the sense of belonging, social interaction, self-identity and competence (Karahanna et al., 2018). However, in terms of protecting information and the public, this has also presented new issues for organisations. For this reason, it is necessary to track shared content on social media sites to find any suspicious material and potential threats. Consequently, there is a need for automated procedures and techniques for keeping track of and evaluating social media information. In 2012, David Omand, Jamie Bartlett, and Carl Miller recognised social media intelligence as an information collecting discipline that could contribute decisively to public safety by providing the public with early warning of chaos and threats (Omand et al., 2012).

Before defining or highlighting the importance, opportunities and weakness of SOCMINT, it is important to first look at the technology of the phenomena, which is social media. A platform that first allowed internet users to post public messages started in 1979 when Truscott & Ellis created the Usenet and a worldwide discussion forum (Kaplan & Haenlein, 2010). However, the era of Social Media as we know it now started about 20 years earlier when an "Open Diary" social platform brought together online diary writers into one community (Kaplan & Haenlein, 2010). The more technology evolved, more popularity concepts like Facebook, Instagram, Twitter and YouTube emerged. The speed of technological change is intimately related to the speed of social change. The modern society is suitably referred to as "liquid" by (Bauman & Haugaard, 2008), as it is always undergoing change. Social media is playing a significant role in major changes occurring in the communication landscape and how people engage with one another. Due to the technological advancement public organisations, such as the police and intelligence agencies, have a duty to respond to and adapt to social changes in communication.

Humans are social beings, few pointers influence the use of social media, for example, self-fulfillment, the need to belong, and the appreciation (Yu, 2013). A study by (Lekhanya, 2013; Ractham & Srisamran, 2018) argues that the use of social media is influenced by people's values, culture, and beliefs. The information provided by social media platforms, especially Twitter and Facebook, has been crucial in assisting the planning of rebellious activities in several Middle Eastern nations, particularly during the 2011 Arab Spring uprisings in Egypt and Tunisia. The Internet Live Stats (2019) estimates that over 4 billion gigabytes of data are

sent each day. As of April 2021, the number of people on the Internet has grown by 7.6% (InternetLiveStats, 2021). This means 60% of the world's population is now online.

In the world of the growing proliferation of the 4IR technologies and data volume on the internet, intelligence analysts, needs to sift through raw data derived from various sources and identify significance, patterns, and warning indicators. The results of the analysis can either produce prescriptive, anticipatory and or descriptive intelligence (Clark, 2020). The intelligence analysis must meet the following essential elements of intelligence, "Who," "What," "When", "Where", "Why" and "How". This is intelligence that either recommends a course of action for decision makers, predicts possible futures, and describe what happened or what is happening. However, the volume of content or information may make the analyst's job challenging, potentially turning this advantage of access to information into a negative. Analysts may discover that they are unable to transform large volume of content into meaningful and quality products for national security. Figure 2 below illustrates statistics that represent the use of various social media platforms in South Africa. Facebook's significance as a SOCMINT content treasure lies in the application's comprehensive approach to social interaction. It is a platform that enables users to share nearly any personal information and preference in a variety of media formats. In-depth discussions, the sharing of photos and videos, the disclosure of geolocation (checking in), and access to buddy networks (unless prohibited) are the results of Facebook. Facebook (amongst several other extremely popular applications) therefore provides intelligence services and agencies with vast volumes of content on all possible indicators with which threat profiles can be constructed (Putter & Henrico, 2022).

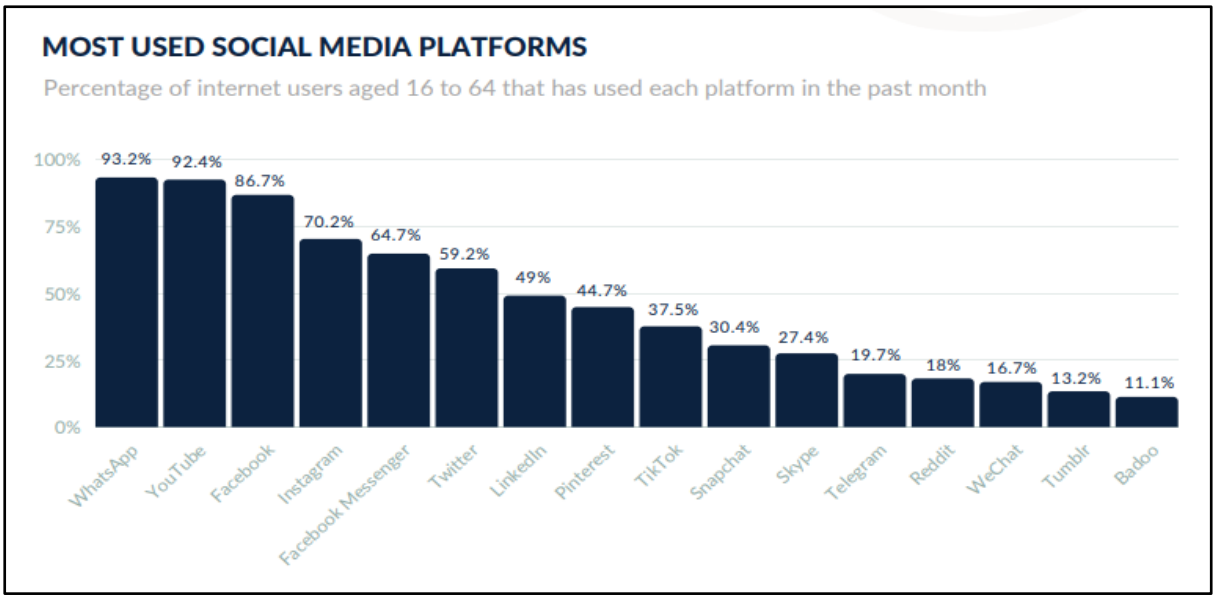


Figure 2. The most used social media platforms in South Africa (Business Tech, 2023)

Millions of postings are uploaded every day to various platforms all over the world, when used properly, these posts can close intelligence gaps, offer real-time situational awareness of events as they occur, and, to a limited extent, provide strategic intelligence (Omand et al., 2012; Bartlett & Reynolds, 2013; Putter & Henrico, 2022). SOCMINT collectors may be interested in a variety of data that may be found on various social media sites. The Facebook profile of a person for an example can be a helpful surveillance tool for the intelligence community. It is possible to track a user through their posts, likes, and shares as well as through a brand-new feature called a "story," which allows users to publish images or videos that may be viewed for up to 24 hours (Howells, 2019). On social networks like Facebook, connections between people can be analysed. Even in cases where friendship is not immediately apparent, it can still be inferred from liked posts or comments. As social network analysis can uncover hidden links in a Facebook network, it would be able to analyse the effect of specific persons over time by analysing the friendships and likes given to posts on Facebook as a network graph (Gilbert, 2018).

Although social media might predict dangers to national security, it can also be used to strengthen national security. For example, the Project Polar investigation, which used shared fitness tracker data to identify secure sites and the geo-positioning trails of intelligence agents, and the Bellingcat investigations into the attempted assassination of Skripal and the downing of Flight MH17 over Ukraine, where the identities of alleged perpetrators and timelines were

fully revealed, are two examples that highlight the effectiveness of social media investigations (Tokmetzis, et al., 2018). Other evidence that demonstrates the opportunities of SOCMINT, was how intelligence analysts successfully leveraged or exploited a leak by a non-complaint ISIS member on Twitter which is a key platform for extremist group's propaganda (Markham, 2015; Berger & Morgan, 2015). As an example of information unintentionally released, an ISIS member boasted in a selfie on Twitter about the "command and control skills for Daesh." The location services linked to the posting allowed Air Force General "Hawk" Carlisle to leverage this information to the US's benefit. It was shown how that piece of location data was used as actionable intelligence when an airstrike was launched and the ISIS building was destroyed after the location had been investigated and verified (Hoffman, 2015). In South Africa, a statement by the Directorate for Priority Crime Investigation (Hawks) stated that a man and a woman, both 35 years old, had been detained in KwaZulu-Natal and Gauteng on suspicion of inciting public violence (Mokoka, 2021). The suspect in KwaZulu-Natal is accused of encouraging public violence with social media and other channels during the turmoil that occurred in the province in July. The second suspect allegedly ran the well-known Sphithiphithi Evaluator (@_AfricanSoil) Twitter account, which has 63,175 followers. In this instance, social media was not used to predict danger to national security, rather it was a reactive and responsive type of approach.

The internet and social media platforms are likely the most powerful communication tools ever created for humankind. This has yielded indisputable benefits to the intelligence community, and it has immeasurable promise or potential for intelligence operations but similarly it has unmanageable communication potential for threats to national security caused by lack of borders, dynamism and anonymity. A recent example is the enormous impact social media has had and continues to have on health intelligence. While governments work to persuade people to get vaccines for covid-19, so-called "anti-vaccine" are using social media to create a false narrative. It is evident that social media can have both positive and negative effect on the spread of information about health issues (Abuhashesh et al., 2021). Gartner IT Glossary, 2018 states that it is exceedingly challenging for intelligence analysts to identify and keep track of all those people who might have an impact on national security because active users are increasing in number and post and share a variety of electronic resources. It is called big data because of "high-velocity, high-volume and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making"

(Gartner IT Glossary, 2018). From this perspective, using social media data mining tools will help to gather timely and pertinent information for intelligence gathering.

2.5 Social Media and its impact on national security

Treverton & Gabbard (2018), argue that intelligence is undergoing a harsh change due to emerging threats because of technological advancements. Technology has created opportunities for cyberattacks, extremist organisations, and criminals, therefore creating a challenge for security and intelligence. Advanced technology is most likely to be exploited to penetrate, manipulate and weaken collection capabilities and social media has enabled that opportunity (Hershkovitz, 2019). The fact that the Arab Springs were organised online suggest that the traditional intelligence collection disciplines were irrelevant. SOCMINT is influencing the political and threating national security to the point where it destabilises social economic activities. It seemed that paying close attention to new media rather than engaging in espionage was the best approach to stay current with significant political changes in history (Britannica, 2021).

2.5.1 The international impact of social media to national security

The Arab Spring serves as an example of how the intelligence community was unable to give pertinent intelligence or forecast the outcome of this event because they were unfamiliar with social media and its use during social movements (Rovner, 2013 & Liaropoulos, 2013). The odd thing about the Arab Spring revolt is that social media was used to voice discontent and to spread the message to other Arab nations, sparking unplanned rallies in a number of those nations. Eventually, violent protests sparked by social media resulted in the overthrow of democratically elected governments in Egypt, Tunisia, and Libya (Ibid). Other significant mass demonstrations that were influenced by social media are Table 1.

Table 1 Significant mass demonstrations

Area	Year	Social Media Unrests
Maldova	2009	Following the Party of Communists' (PCRM) victory in the legislative elections held in April 2009, there was widespread civil unrest. The opposition accused the PCRM of fraud, which caused protests

Iranian election protests (Great Revolution)	2009–2010	Young Iranians staged a social protest following President Mahmoud Ahmadinejad's re-election by alleging that the elections had been manipulated. The Iranians used social media throughout this movement, mostly Twitter, to spread information about the protests. Due to Iran's extensive digital surveillance and internet control, social media sites were blocked during the rebellion, and intelligence agencies were able to identify those who were encouraging the protests (Aday et al., 2010).
Tunisian Revolution (Jasmine revolution)	2010–2011	Mohamed Bouazizi, a 26-year-old fruit and vegetable vendor who set himself on fire, gained attention from all around the world thanks to social media (Safranek, 2012). Social media platforms were used to share photos and videos of Mohamed's act and to Tunisians who had internet access as well as with people all over the world.
London	2001	When Mark Duggan was fatally shot by the police on August 4, 2011, there was widespread outrage in England (HMICFRS, 2011 & SAS, 2012). The protest organisers used social media during this period to coordinate their activities and mobilise residents. The police's attempts to put an end to the protests were hampered by their inability to fore warn because the civil unrest demonstrators always outpaced them.

Another recent instance of social media providing both tactical intelligence and forewarning is Russia's gathering of forces on the border with Ukraine in March 2021. Residents in western Russia shared videos and images in enormous quantities of military soldiers and vehicles moving in the direction of Crimea. The Crimean locals kept track of the whereabouts and movements of these resources close to the border (Vandiver, 2021). This was a day after US European Command released its state of readiness to “possible impending crisis” (Simferopolnovosti, 2021). TikTok was,

possibly for the first time used for a conflict-like situation and a very potent intelligence gathering platform (Johnston, 2021). This was a sign of the constantly expanding growth of social media. TikTok users would immediately send footage to the app as they saw trains carrying tanks and other armoured equipment, or as they drove past columns of soldiers. TikTok became a crucial tool for tracking Russian activities in South Western Russia (Johnston, 2021).

2.5.2 **The South African impact of social media on national security**

According to Stegen (2019), the use of social media in South Africa relative to the threats discussed above, two threats were observed:

2.5.2.1 The use of social media as a propaganda tool: Bell Pottinger's propaganda effort is a prime illustration of this type. The Gupta billionaires funded a campaign of misinformation to divert attention from claims of state capture and released by the Public Protector (Cherian, 2021). The clandestine initiative, created by the public relations giant Bell Pottinger, entailed inflaming racial animosity with a narrative of "white monopoly capital" (Wasserman, 2020). Bell Pottinger used social media campaigns to plot their narrative. The people of South Africa felt the campaign's primary effects. The results of the champagne were a rise in racial tension.

2.5.2.2 Protest movements and revolutionary threats: Students from the University of Cape Town launched the RhodesMustFall campaign in January 2015 in an effort to remove Cecil John Rhodes' statue. (Kwoba, 2018; Chigudu, 2020). In response to this protest, the statue was taken down in 2016 (Chigudu, 2020). #FessMustFall is another movement that was mobilised through social media (Lang, 2017; Malumba, 2017). In opposition to the proposed rise (11%) in tuition fees, the #FeesMustFall movement began at the University of the Witwatersrand (Wits) in October 2015 (Lang, 2017; Breakey, 2017). Other universities in South Africa quickly adopted the initiative. President Zuma responded to the demonstrations by announcing that there would not be a fee rise for the 2016 school year (Breakey, 2017). Collectively, these became the largest student social movements since the dawn of South African democracy in 1994 (Habib, 2019).

The incidents discussed above, prompted the then Minister of SSA to initiate an investigation in the regulation of social media (Tavani, 2017). However, five years later, the South Africa intelligence community has not used SOCMINT to its full potential and South Africa still does not have the SOCMINT legal framework to regulate the use of social media.

2.5.3 South Africa's response to the July 2021 unrest

The intelligence agency seemed unable to process the information that was spreading through social media during the July unrest. WhatsApp, Twitter, and Facebook seemed to be the most dominating social media platforms to spread the information (Civil unrest report, 2021). According to O'Regan (2021), to respond to the violent protests and looting that occurred in the province in July, KwaZulu-Natal Premier Sihle Zikalala and his administration turned to social media, news stories from the mainstream media, and an online booklet warning of a shutdown. Testifying at the South African Human Rights Commission's (SAHRC's) public hearings, the Premier Zikalala told the commission that "before the outbreak, there was no information received from any crime intelligence structure on the imminent threat in KwaZulu-Natal indicating its context, nature and the need to prepare the security clusters response accordingly," (SAHRC, 2021). The intelligence scholars like Copeland (2004) and Jervis (2006), states that lack of information sharing from various intelligence communities have limited the effective use of technical collection methods, therefore impacting national security.

According to Lowenthal & Clark (2015), the barriers of information sharing impact the effective use and is affected by the internal competition between different intelligence communities in a country. This problem was evident during the 2021 civil unrest in South Africa. The South African intelligence agency is known for its controversial use of covert, intrusive and secret methods, but they were criticised for failing to forewarn the police of the impending violence. South African Police Service (SAPS) were criticised for reluctance to respond. According to the report by the expert panel into the July 2021 civil unrest, it is understood that the SAPS's response to the impending violence was not effective because they did not have the intelligence upon which they could have planned their operations. Thus, information sharing could have played a key role in the unrest. A variety use of different intelligence processes could help prevent future intelligence failures.

O'Regan (2021) and Mokoka (2021), states that the Centre for Analytics and Behavioural Change (CABC), a non-profit organisation founded to monitor and combat false information,

disinformation, and polarising rhetoric online, identified 12 Twitter accounts that were crucial to the unrest after it broke out in KwaZulu-Natal and Gauteng. The accounts belonged to the RET forces network (Mokoka, 2021), as demonstrated in Figure 3 below, CABC found that several hashtags were meant to incite unrest through, among other techniques, calling for shutdowns around South Africa (Mokoka, 2021).

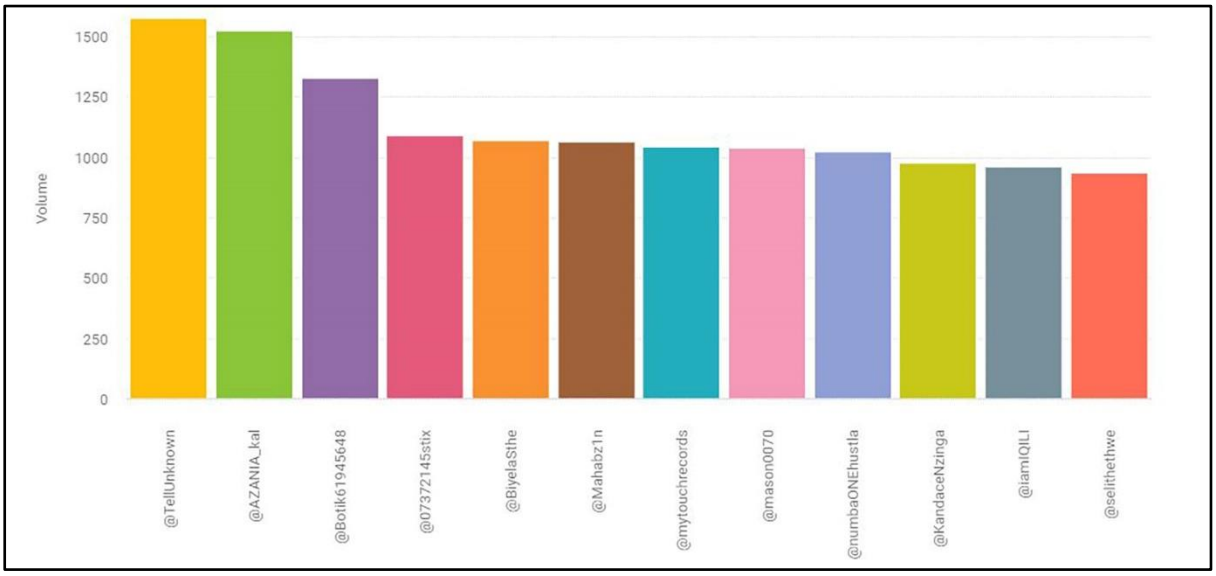


Figure 3. Top 12 accounts belonging to RET network (Mokoka, 2021)

Although some academics like Eaton (2013); Howard et al. (2013) and Liaropoulos (2013) agree that social media may not start the revolution, they do claim that it does help to support and facilitate protester's efforts to democratise society. Morozov (2011), disputes the idea that social media may spur protests and ultimately lead to community democratisation. Instead, he sees the social media platforms as tools or instruments in the hand of government or security services since they can be used to gather intelligence about social movements (Morozov, 2011). His argument concurs with Howard (2013) and Liaropoulos (2013); Thompson (2011), that social media amplified the effectiveness of protests even though it may not the cause of the unrests. For example, in the South Africa's July 2021 civil unrest, social media was only a tool that instigated the situation due to the underlying socio-economic and political conditions of the country.

All the incidents discussed above have a common theme of attribution of challenging 'mainstream' realities and narratives through network enabled and social media activism (Sunstein, 2016). However, because the literature has not yet developed an adequate

understanding of how these messages transfer into real-world action, it is still impossible to evaluate if the social media interventions or dynamics in those cases were compelling or persuasive. Fearing the repetition of the July 2021 unrest, the intelligence community and other security clusters were better prepared with the March 2023 Economic Freedom Fighters (EFF) 'national shutdown'. The EFF announced a "national shutdown" on Monday 20 March 2023, sparking concerns about looting and violence. The shutdown was officially announced through media houses and different social platforms. In response to the announcement, the National Joint Operational and Intelligence Structure (Natjoints) which comprise of SSA, SAPS, National Intelligence Coordinating Committee (NICOC) and other core members of the security cluster had put measures in place to combat any forms of criminality. Given their poor communications and failures during the violent and economically damaging riots of July 2021, security services and the government provided citizens regular information about the shutdown. To stop possible violence and looters, the SAPS, private security, community policing forums, and neighbourhood watches worked together and shared information that would impact national security. In a media statement by the African National Congress (ANC), "there was absolutely nothing revolutionary about the EFF march, but rather a populist effort that seeks to promote lawlessness and a feeble attempt to invoke the Arab Spring Revolution mindset" (Davis, 2023).

One can argue that the intelligence community and security cluster were successful in preventing criminality during the March 2023 "national shutdown" compared to the July 2021 unrest. In the March 2023 shutdown, there was prior announcement by the EFF, thus the Natjoints could better prepare for possible unrest. Yet again, before the July unrest, political tension started to intensify in KZN when President Zuma appeared before the Judicial Commission of Inquiry into allegations of fraud and corruption. On 29 June 2021, the president was sentenced to 15 months in prison, and he was expected to submit himself to the SAPS in Nkandla. Thus, his sentencing was a major build up to the violence and looting that took in July 2021 (civil unrest, 2021). Despite NICOC's early predictions that 2021 would be a very volatile year, the National Security Council had not been meeting regularly before unrest July 2021. This is troubling because it was evident that there was increased mobilisation for protests and that there were intermittent violent protest outbursts throughout the first half of the year (civil unrest, 2021). Therefore, the national community and security cluster had knowledge of potential mobilisation as much as they had knowledge of the March 2023 "national shutdown", thus, they should have responded swiftly as they did with the March 2023 shutdown. It is

important to draw lessons from other intelligence services who might have experience and dealt with similar political unrests.

2.6 Lessons to be learnt from intelligence failures

Many academic experts on the Arab world shared their general public's amazement at the upheavals that led to the overthrow of two Arab governments. Until 2011, the Arab world was boasted with persistence undemocratic rulers (Rezk, 2017). The dictator leadership resulted in revolutions in Egypt, Tunisia and Libya. In the wake of the uprising, there has arguably been propensity among the intelligence community to dismiss claims of intelligence failure by characterising revolutions as mysteries (an unforeseen event) (Hayden, 2011; Ambinder, 2011). According to Gentry & Betts (2019), warnings about political upheavals remain essential for the intelligence organisations, therefore, cannot be recorded mysteries. The Arab dictatorship was attributed by two factors, state control over the country and military security complex, hence the eventual revolution (Gause, 2011; Rezk, 2017).

A study by Stenslie (2023), examined why the Norwegian Intelligence Service's (NIS) in the Middle East was unable to anticipate the outbreak of the Arab Spring, and the lessons can be drawn that can put the intelligence community in a better position to warn of future revolutions. The investigation by the Norwegian Intelligence Services focused on the following observation:

2.6.1 Direction speaks of the dialogue between the producer and the consumer of intelligence that determines the priorities for a certain service. In the early 2000s, the war in Iraq and Afghanistan and the coming up threats by al-Qaida made counterterrorism operations a priority for NIS (Johansen, 2011). As a result, resources were channelled to counterterrorism operations and political developments and trends were neglected (Stenslie, 2023). Even the CIA, a service one would typically assume to have practically limitless resources, did not have an analyst specifically focused on Tunisia, the country where the upheaval first started (Lowenthal, 2019).

2.6.2 Collection, intelligence collection disciplines and data processing. NIS analysts look for indicators of change, such as signals and trends. They were heavily involved in elite and great power politics while mostly ignoring civil society and the public (Wankhade et al., 2022). The issue surrounding the Muhammad cartoons might have functioned as

a warning to Norwegian and other Western intelligence services about the impending political unrest on the "Arab Street" (Dilanian, 2012). Nevertheless, it was largely disregarded as a significant political factor. According to Stenslie (2023), social media platforms we underutilised resources to gather information and capture the political sentiments of the people in the Arab nations. Wankhade et al. (2022) and Stensile (2023), state that the main task of NIS open sources analysts was to keep an eye on traditional news sources and there was minimal effort made to track changes in population attitude, a crucial sign that political unrest may develop.

2.6.3 Processing, data that is systematised, analysed, and summarised into an intelligence product. Experts do a fantastic job of explaining why things are the way they are, but they struggle with making future predictions (Tetlock & Gardner, 2005.). The approach preferred by intelligence analysts is indicator-based warning analysis, but the method has limitations when anticipating a revolution (Gentry & Gordon, 2019). The Failed Stated Index is an annual report mainly published and supported by the United States think tank the Fund for Peace. It assesses 178 countries based on a measurement of the social, economic, and political pressures that each country faces (Fund for Peace, 2023). According to the 2010 index, 2011 may have seen unrests in Yemen but not so much in other Arab nations (Goodwin, 2011).

There is no guarantee that any intelligence agency will be able to predict the next revolution. It takes tremendous intelligence to foresee such an occurrence. However, one cannot merely concede that revolution is an uncontrollable "mystery." Therefore, it is essential to draw lessons from the past, adapt the work to the goal, and find and implement new and pertinent techniques and method. One way of implementing new techniques and methods is through SOCMINT. The South African government missed the opportunity to defuse and disrupt the planned violence and they did not leverage the power of social media. Some of the opportunities that could have been used by the South African government are presented in the next section by Omand et al. (2017) and Montagnese (2012).

2.7 SOCMINT Opportunities

Leveraging the power of social media for security reasons can be challenging and without the right expertise, skills, tools, and technology, it is next to impossible to successfully monitor the platforms and timely response to possible threats. Social media threats that affected national

security were demonstrated in the above-mentioned incidents, however Omand et al. (2017) and Montagnese (2012), presented the SOCMINT opportunities that can mitigate the threats:

2.7.1 Crowd-source information: this refers to a situation where there is a great exchange of information between the public and government institutions, particularity during times of emergency (Omand et al., 2017). In a crisis, the general people could use crowdsourcing to provide real-time updates on what is occurring locally. Ushahidi (www.ushahidi.com), an open-source disaster map tool developed in 2007 and is used in places like Kenya, Mexico, Afghanistan, and Haiti. The platform serves as an example of an effort to use crowdsourcing to aid the humanitarian community in enhancing cooperation. It makes use of Web 2.0 technology to combine data from various sources, including mobile devices, websites, email, and social networking sites like Twitter and Facebook, to produce an up-to-date disaster map that is accessible to the public and is also available to relief agencies (Gutierrez, 2018).

2.7.2 Research and Understanding: Studying social media could help people better comprehend a range of issues involving behaviour and social interaction, particularly radicalisation. Social media surveillance will help the security environment identify warning indicators of hostile or potentially dangerous activity and provide forewarning to government. Social media research can be accessed through 'open source,' which is data obtained from Twitter and other social media content made available for public access. However, some of the data will need legal consent to overcome privacy settings and communication encryption.

2.7.3 Near real-time situational awareness: Social media can help paint a picture of how events are developing. With the utilisation of geo-location, this may result, for instance, in a continuously changing map displaying surges in potentially violent tweets map that displays spikes in tweets enabling a quicker more efficient, and more agile emergency response.

2.7.4 Insight into groups: This would include having a better understanding of the actions and conduct of specific groups that are already of interest to law enforcement or intelligence authorities. Terrorist organisations employ internet-based communication tools to disseminate their ideology, recruitment drives, and propaganda, claim

(Theohary & Rollins, 2011; Montagnese, 2012). The primary medium used by terrorists is social media (Helmus et al., 2013; Moe & Schweidel, 2014).

2.7.5 'Geofencing' technology (such as 'Geofeedia') allowing to locate and manage near real-time threats (Dabhi, 2016).

Because there are so many SOCMINT opportunities, the Russian National Guard (Rosgvardia) was preparing and training Russian Army experts as SOCMINT operations specialists (Golts, 2017). The National Guard was established in response to the threat posed by so-called non-violent resistance methods, the commander in chief of Rosgvardia stated bluntly (Golts, 2017). Considering this, the Russians claim that SOCMINT offers a reliable source of information that might be applied to the actual identification of national security threats. Both South Africa and Russia are BRICS members. As a result, the BRICS alliance serves as the ideal means of global cooperation for the exchange of knowledge on SOCMINT. Since SOCMINT has proven to present reliable information to identify national security threats, it should officially be recognised as an intelligence collection discipline with its own standards of evidence, dedicated expertise and technical methods. All these methods need to be understood, and they are discussed in the next section.

2.8 SOCMINT as an intelligence collection method

Emerging technologies are already reshaping how SOCMINT gathers, stores and process information. In Table 2, Bartlett and Miller (2015), presents SOCMINT intelligence collection methods that can improve decision making to prevent, pursue, protecting, and preparing against terrorism.

Table 2 SOCMINT intelligence collection methods

SOCMINT collection methods	Description
Data mining and predictive analytics	Statistical analysis of large data sets on social media to find connections and interactions.
Natural language processing	A field of artificial intelligence that involves the computational study of "natural" language as it appears on social media, frequently utilising machine learning techniques. It is a method of

	gathering and managing enormous "natural language" data sets, such as those from social media.
Named Entity Recognition (NER)	A framework was proposed by Le Sceller et al. (2017) for automatic detection of cyber security events over the twitter stream. This technology classifies tweets according to their relations.
Manual analysis	Netnography is the "application of ethnographic and qualitative sociologies to the study of social media" (Bartlett & Miller, 2013).
Event Detection	This technique detects or discover planed offline events, be they political, cultural, emergency, and economical to offer situational awareness
Social network analysis	It is possible to identify characteristics of the network structure, the topology of the network, and the type of network, by using applications based on mathematical techniques (Kadushin, 2012).
Web scrapers and crawlers	These are automatic algorithms that are used to locate and compile data kept on websites. The links to the sites are recorded by crawlers as they trace hypertext links from one site to the next.

With modern technology, Ingle (2023), presents capabilities used to gather data from SOCMINT open sources. Some of the latest SOCMINT collection methods in the modern society are presented in Table 3.

Table 3 Modern SOCMINT Technology

Modern SOCMINT technology	Description
Intel 471	This is a free SOCMINT espionage program capable of gathering and analysing variety of data, including IP addresses, CIDR ranges, domains and subdomains, ASNs, email addresses, phone numbers, names and

	usernames, and even Bitcoin addresses (Koloveas et al., 2021).
SEON	In today's digital economy, using a person's social media and other online accounts to verify their identity is becoming more commonplace. SEON has taken the lead in digital identity verification (Koenig, & Murray, 2022). Organisations can use SEON to implement queries directly, through an application programming interface (API), or even via a Google Chrome plugin.
Lampyre	SOCMINT open-source focused software that provides efficient assistance with tasks like due diligence, cyber threat intelligence, criminal investigation, and financial analytics (Daskevics & Nikiforova, 2021).
Spyse	Is the "largest comprehensive internet assets registry" for cyber security specialists. Spyse is a data gathering platform that is used by several organisations, including IntelligenceX, OWASP, and Intel 471. The Spyse engine then analyses this data to spot potential security threats and determine connections between the relevant entities (Böhm & Lolagar, 2021).

According to Bartlett and Miller (2015), the use of SOCMINT is more promising for the purpose of counting terrorism. Natural language processing for an example is most likely to be helpful in counterterrorism content during or immediately following a terrorist occurrence (Barlett & Miller, 2015). Nowadays, there is always a lot of social media activity that goes along with big events. Analysts can swiftly and accurately identify and interpret critical information as it is posted thanks to natural language processing, which is helpful for intelligence gathering and quick response (Böhm & Lolagar, 2021).

The discussions above clarified the significance of SOCMINT and the methods for gathering and using information. However, one must be aware that SOCMINT does face challenges that must be considered. This is discussed in more detail in the next section.

2.9 SOCMINT Challenges

Social media undoubtedly makes it more difficult to sort through all the information available because there are so many social networking sites and so many people on each of them. Facebook has more than one billion users, while Twitter has an average of 307 million users (DataReportal, 2022). Social media exacerbates the problem of information overload that intelligence services already experience in this way (Hershkovitz, 2019). The process of sifting through the abundance of information available is highly time and money consuming. According to Hershkovitz (2019), from 1995 to 2016, the amount of reading required of an average US intelligence researcher (in a low priority country) grew from 20 000 to 200 000 words per day. The volume of content on social media makes it challenging for intelligence analysts to find common patterns and trends in data.

It is important to understand that SOCMINT's ability to prevent national security threats does not rest on the methods employed by the intelligence communities to protect the society, but it also lies on the public's involvement and accessibility. The National Security Strategy of Britain acknowledges that effective security and intelligence operations depend on people and communities working together actively as well as on public understanding and consent (Tannam, 2017). As Pallaris (2008), states, "the promises made by technology vendors, no matter how sincere, they cannot replace the enormous analytical effort that the wealth of OSINT requires from human beings" (Byrne, 2015). According to Moffet (2021), human collectors can offer insight into the human perspective while technical intelligence gathering disciplines are restricted to assessing human intention capabilities.

As new channels enabling terrorist group members to interact with one another without being discovered by law enforcement or intelligence community, social media makes the job of intelligence analysts more challenging (Charania, 2016). For instance, ISIS makes use of Telegram, a safe mobile messaging software that provides an option for "secret chats" with messages that are encrypted. Before the incident on December 6, 2015, the organisation had posted a Telegram call to target Saudi and Emirati forces in Aden (Huggle, 2016; BBC News, 2015). Furthermore, according to Omand, Bartlett, and Miller (2012), Before SOCMINT can be used effectively for national security and public safety, several significant issues must be resolved. According to the authors, these difficulties include ensuring that social media information is used effectively, that decision-makers value social media information, and that the public approves the use of such information for security and public safety objectives. This

is due to the possibility of privacy invasion while accessing publicly available information on social networking networks (Solove, 2018).

Beyond all of this, determining the boundaries between what is public and what is private, as well as issues of confidentiality and consent, privacy consideration and regulations are the biggest obstacles and challenges that pertain to the use of SOCMINT.

2.10 Legal, Ethical and Privacy consideration

In the second half of the 20th century, concerns about securing one's personal information, which is now easily gathered, stored, and shared amongst electronic systems, have come to increasingly dominate discussions about privacy (Tavani, 2015). The significant correlation between privacy and personal information is due to several factors, including the rapid advancement of technology and the rise of social media. Solove (2008) critiques what he refers to as the "reasonable expectation of privacy method" to addressing and defining privacy interests since it leaves room for platform providers, common co-users, or authorities to gather, derive, generate, or produce new personal information. Given the nature of social media platforms, it is important to determine to what extent people's privacy can be protected.

The legal protection of privacy in the context of social media appears to be confusing and, in some situations, limiting for international intelligence organisations (Ronn, 2019). Given that these organisation's mandate is to alert or fore-warn the government about impending security threat. In these conditions, the concept of privacy in the online environment has been challenging (Ivan, 2015). The biggest SOCMINT issue arises when someone intrudes into another person's personal space or when an intelligence officer uses intrusive techniques to gather data and information. Thus, it is important to have legislative framework or regulations that govern the use of SOCMINT. According to Omand et al. (2012), "The 'successes of intelligence is not the information or even secrets that it collects, but the value it adds to decision-making". As a solution to resolve the issues of privacy and legal framework, six guiding principles were developed by Omand et al. (2012), in relation to intrusive SOCMINT:

2.10.1 An analyst who gathers data must have a good and legal justification before engaging in intrusive activities that violate several privacy laws. The national security interest and the prevention of a phenomena that violate national security grounds and involve

the maintenance of public order and safety are the most compelling arguments that can be made (Omand et al., 2012).

2.10.2 An integrity plea, there is an argument that every action made must have a justification at every point of the intelligence cycle.

2.10.3 The justifications for using such the SOCMINT techniques must adhere to the proportionality and necessity criteria. Thus, the usage of intrusive techniques must be minimal and efficient if used.

2.10.4 The development of a legal framework that governs any action that compromises a person's online privacy and confidentiality.

2.10.5 This type of intelligence gathering must only be employed as a very last resort.

2.10.6 This intrusive method must have a favourable outcome.

SOCMINT calls for more particular rules, guidelines, and safety measures that take into consideration the incredibly special and distinct nature of social media, which is a privately-owned (controlled by private enterprises) environment where people are free to communicate (Ronn, 2019). According to Bartlett and Reynolds (2015), most Organisations for Economic Cooperation and Development (OECD) countries have legislatives that covers the collection and use of confidential information that are meant to ensure that government agencies can only access people's private data in a legal way. Legal frameworks in different countries are based and supported by different principles. For instance, in the United Kingdom (UK), the gathering of information that could be regarded as "private" involves the use of a stringent authorisation process, oversight by legitimate entities, and that the intelligence is used for appropriate objectives and obtained using appropriate techniques (Briggs, 2017). In the UK, a Regulation of Investigatory Powers Act (RIPA) authorisation is necessary whenever there is a chance that "private information" will be obtained (Briggs, 2017). In Belgium, whether "technical methods" are employed, it affects the requirement for a judicial or departmental warrant (Omede, 2015). African nations, like Nigeria, have laws governing social media, but these measures have drawn criticism for violating human rights (Omede, 2015).

2.11 Regulation of SOCMINT in South Africa

For the intelligence community in South Africa, social media is a new source of intelligence that both poses threats and offers opportunities. Thus, it is crucial to create a theoretical and

strategic framework that incorporates SOCMINT to mandate and direct the use of this intelligence source inside the intelligence environment. Since SOCMINT is not included in the South African intelligence framework (Stegen, 2020; Putter & Henrico, 2022), the following questions should be considered in this regard: *Which South African laws affect the use of SOCMINT by the country's intelligence services and organisations?*and *is there clear guidance in SA law regarding the application of SOCMINT for domestic national security?*

The National Strategic Intelligent Act of South Africa requires the National Communication Centre (NCC) to conduct international intercepts SIGINT (National Strategic Intelligence Act, 1994). The intelligence technique used to intercept satellite communication is known as Signal Intelligence (SIGINT) (Ball, 1989). The only law that controls domestic communication signal interception is the Regulation of Interception of Communications and Provision of Communications-related Information Act (RICA). Despite having a foreign intelligence mandate, the NCC has come under fire for being used improperly to spy on South Africans over the years. As of right now, there is no legislation regulating NCC to intercept signals inside South African territory.

The intent of RICA is clear, it is intended to give the state extensive legal protection to conduct intelligence operations in the SIGINT and SOCMINT domain (Republic of South Africa, 2021). Additionally, RICA aims to control how intelligence services and agencies conduct their operations. However, the regulation was found wanting by the constitutional court in February 2021 ruling that RICA was unconstitutional (Duncan, 2021). The court claimed that it did not offer "sufficient protections to protect the right to privacy." This came after the South African Constitutional Court shut down the NCC's international SIGINT capabilities for South Africa (Duncan, 2021). Over the years, the NCC has been charged with violating its mandate because of political abuse and influence. The court's ruling stated that the NCC's actions were illegal because no legislation was in place to regulate them for domestic interceptions (Duncan, 2021). The Constitutional Court's decision establishes a precedent for intelligence operations including SOCMINT domain and would preferably want SOCMINT operations to be a last choice of intelligence gathering due its intrusive nature.

In South Africa, if personal information is in the public domain, no warrant is required to get it (Swart, 2018). However, it is prohibited to intercept any communication that is not in the public domain without the consent of a court assigned to explicitly decide on all interception

applications, in accordance with the RICA (70 of 2002). However, in line with RICA, it is illegal to intercept any communications that are not in the public domain without the approval of a court designated to specifically decide on all interception applications (Swart, 2011). South Africa's intelligence communities are required by law to provide state decision makers with pertinent and timely intelligence that may threaten national security. One important content source that is growing in importance is SOCMINT because it has a potential to produce the intelligence products needed to make informed judgments on national security. Thus, the Intelligence Strategic Intelligence Act 39 of 1994, describe the functions intelligence organisations. The intelligence mandate does not describe or deal the type of approach or the manner (collection discipline) in which intelligence should be gathered, thus it is assumed that all the intelligence collection discipline's (SIGINT, HUMINT, GEOINT, IMINT, OSINT AND SOCMINT) content will be used to assess the threat.

Other South African regulations that affect the usage of social media and their monitoring is the Crime Procedure Act 51 of 1997. The importance of the Criminal Procedures Act comes from the authorisation of monitoring and surveillance of individuals. The act also covers the monitoring of certain social media accounts (Criminal Procedure Act, 50 of 1997). According to the Criminal Procedures Act (51 of 1977), any law enforcement or intelligence agency can request access to cell phone records, telephone records, or details regarding cell phone ownership and billing by applying to a magistrate, regional court magistrate or high court judge (Swart, 2011). For example, if a fake account is necessary for clandestine operations, the Act is applicable (Swart, 2018). Considering the threat to national security, the question of whether the right to privacy is more important than the "well-being of the nation" still stands. Thus, from the perspective of national security threat, it is still a question of the right to privacy and whether that right carries greater weight than the "well-being of the nation.

2.12 Theoretical Framework

To better understand adoption of technology in organisations, it is important to look at proposed theories of technology adoption and acceptance. Several adoption theories include Technology Acceptance Model (TAM), Diffusion of Innovations (DOI), Unified Theory of Acceptance and Use of Technology (UTAUT), Theory of Planned Behaviour (TPB), and Technology Organisation-Environment (TOE) framework. The adoption of technology at the human level was primarily examined using the theories TAM, UTAUT, and TPB, whereas the adoption of technology at the organisational level was examined using the theories DOI and TOE (Halawi

& McCharthy, 2006). Since this study attempts to investigate the SOCMINT adoption at the organisational level, the following sub-sections discusses the principle of technology adoption theories at the organisational level, DOI and TOE framework.

2.12.1 Diffusion of Innovations

Diffusion theory was created for farming technologies, but it has since been adapted and applied to many other fields and technologies, yielding a method that is methodologically and empirically established (Rodgers, 1976). The theory is frequently used to explain IT innovation adoption, including how, why, and what the adoption rate is (Rodgers, 1976). The DOI theory is concerned with how innovations spread through time among the individuals in a social system. Adopters, who might be an individual, a group, or an organisation, make up the social systems (Haneem et al., 2019). Perceived benefits, compatibility, complexity, trialability, and observability on the adopters are among the technological elements of IT innovation adoption that DOI theory offered (Haneem et al., 2019).

Although DOI theory has a strong theoretical base and consistent empirical support in the literature on IT innovation adoption, the previous researchers have made significant criticisms of its relevance in explaining adoption at the organisational level (Lundblad, 2003). The idea of innovation diffusion wasn't developed by looking at any high-end technology products; rather, it has its roots in the agricultural fields (Ryan & Gross, 1943). The theory was initially criticised for its dominance in the agricultural environment and unsuitable for advancements in other areas, which was its main point of contention (Wani & Ali, 2015). This is because when researchers started to study the adoption patterns of farmers using hybrid corn, they adopted the innovation diffusion theory (Wani & Ali, 2015). The business community also spoke out against the theory, arguing that categories of adopters are not fixed throughout time (Garcia-Aviles, 2020). Anyone can innovate if their ideas are paired with organisations who are interested in adopting them. Because a key component of Rodger's adoption model relates to how the technology is perceived, DOI theory has been criticised for being techno-deterministic (Rodgers, 1976). However, Rodger maintained that his model views innovation as a process of communication whereby individuals of a social system communicate information to arrive at a shared understanding of the technology (Garcia-Aviles, 2020). Lee & Cheung (2004) concurred with the criticism stated that DOI ignores the impact of organisational and environmental factors when examining the technology adoption. Therefore, it is argued that DOI theory by itself is less appropriate for understanding IT innovation

adoption at the organisational level. Baker (2012) claims that with the development of the TOE framework's technological dimension, DOI theory is consistent with it.

2.12.2 Technology Organisation-Environment (TOE)

In a review study, Oliveira & Martins (2011), examined the theories that have been used to explain key factors influencing the adoption of IT innovations at the organisational level. The study thoroughly analysed earlier research on the adoption of IT innovations that had used the TOE framework as their guiding theory. Due to the TOE framework's strong theoretical foundation, consistent empirical support, and flexibility in specifying the variables under each proposed dimension, it was often employed in IT innovation adoption research (Haneem et al., 2019). Furthermore, Tornatzky & Fleischer (1990), developed the TOE framework. TOE was utilised by Salwani et al. (2009), to look into how tourism enterprises utilised e-commerce, and by Hoti (2015), to look into information systems. Additionally, TOE has been used to explain the adoption of corporate systems, social media, and IT (Chao & Chandra, 2011; Wamba & Carter, 2014). All of this earlier research has demonstrated that environmental, organisational, and technological aspects all affect how people decide whether to adopt new technologies. Tornatzky and Fleischer (1990), identified three factors of an organisation's context that have an impact on how it adopts and applies technological innovations. These contextual factors are explained below (Tornatzky & Fleischer, 1990):

2.12.2.1 Organisational factors: is a term that relates to descriptive characteristics of the organisation, such as its size, scope, managerial structure, information sources and communication channels, degree of centralisation and managerial beliefs (Eze et al., 2013; Kannabiran & Dharmalingam, 2012).

2.12.2.2 Technology factors: refers to both internal and external technologies that are pertinent to the organisation. This comprises the organisation's present procedures and tools, as well as the range of externally accessible technology (Huang et al., ` 2008).

2.12.2.3 Environmental factors: refers to an environment in which an organisation operates. There are many environmental factors proposed by scholars. Amongst others, the legal system, the government and its agencies, legislature, and professional groups are a few of the factors that influence technology adoption. Economic and financial systems, as

well as state laws and policies, have an impact on how innovations are adopted (Landsbergen & Wolken, 2001).

This study adopted the TOE framework as the underlying theory in categorising the drivers of IT innovation adoption in a context of intelligence organisation due to the restriction of DOI which ignores the influence of organisational and environmental factors to the adoption of IT innovations. TOE has received significantly more substantial empirical and theoretical validations in the information systems (IS) field (Yoon & George, 2013; Zheng et al., 2011). However, it was accused by Ven and Verelst (2011), of not providing particular information and instead using taxonomies to group elements into contexts. The TOE model identifies three important aspects of an organisation that influence the process of technology adoption and implementation (Tornatzky & Fleischer 1990), namely, *technological context*, *organisational context* and *environmental context* as discussed above. Yoon and George (2013), suggest that TOE should incorporate different adoption theories that indicate individual contexts to categorise factors into adoption contexts and determine the underlying linkages among them. The TOE framework rarely explicitly embraced individual characteristics, despite the work of scholars (Awa et al., 2011; Haneem et al., 2019). To influence IT adoption, technology's usefulness and ease of use influence an organisation's strategy, motivation, and attitude. Therefore, the theoretical capabilities of the TOE are extended by including Venkatesh et al., (2007), Unified Theory of Acceptance and Use of Technology (UTAUT) to deal with decision makers' characteristics.

2.12.3 The Unified Theory of Acceptance and Use of Technology (UTAUT)

Since the 1970s, attention has been drawn to information system's adoption, acceptance, and usage behaviour as a component of software quality activities in the field of software engineering as a first step for the utilisation and manifestation of technologies (Momani, 2020). Understanding the reasons why organisations accept or reject any new technology has now become a crucial responsibility in the life cycle of any information system (Sivathanu & Pillai, 2019). Technology acceptance theories like the Unified Theory of Acceptance and Use of Technology (UTAUT) is one of the powerful theories that was created to study how well people could accept technology and how likely they were to adopt new technology (Momani, 2020). Venkatesh et al. (2003), created UTAUT as a thorough synthesis of earlier technology acceptance research based on a review of the existing literature.

Performance expectancy, effort expectancy, social influence, and facilitating conditions are the four main constructs identified by UTAUT that affect behavioural intentions to use technology. The research adopts these constructs and definition from UTAUT to the SOCMINT adoption and use by the intelligence community. Here, *Performance expectancy* is the extent to which utilising SOCMINT will assist the intelligence community; *Effort expectancy* refers to the degree to which the intelligence community believe that utilising SOCMINT would be effort free and easy to use; *Social influence* is the anticipated impact of others on the user's decision to begin and continue utilising SOCMINT (others include bosses, peers, subordinates); *Facilitating Conditions* refers to how intelligence communities perceive the tools and support at their disposal for carrying out a behaviour (Venkatesh et al., 2003). Additionally, it is hypothesised that individual differences, such as age, gender, and experience, will influence a variety of UTAUT interactions (Venkatech et al., 2003).

2.13 Factors that influence technology adoption

Intelligence studies is a relatively young discipline and theories unique to the field of SOCMINT are yet to be developed. The paper proposes a framework that integrates TOE with UTAUT framework. Figure 4 below illustrates the TOE as the study's proposed conceptual framework. The characteristics of individual adopter are captured by the UTAUT theory (Venkatesh et al., 2007).

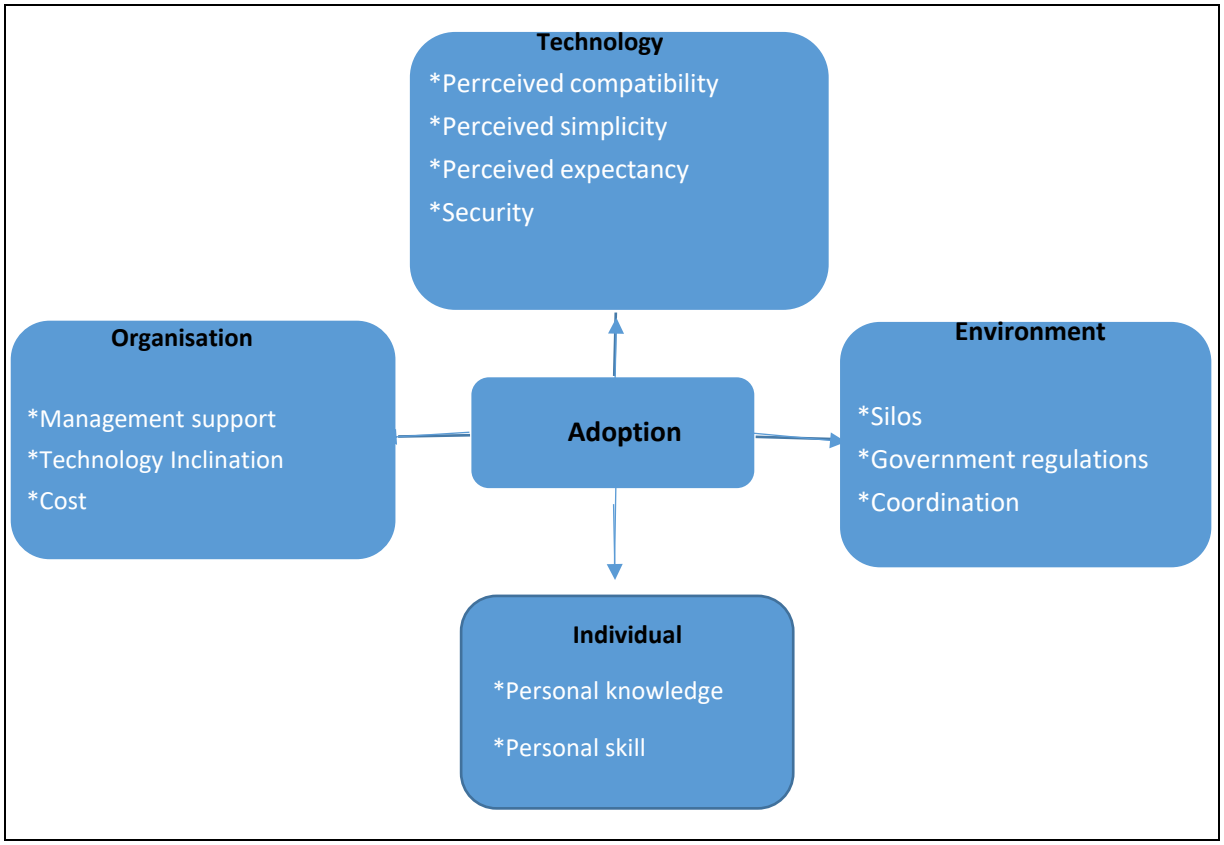


Figure 4. The proposed conceptual framework

2.13.1 Technology Factors

There is not much information accessible in South Africa about technological advancements within the intelligence services. Due to the nature of the information and the method it is acquired, technology used by the intelligence services is of a very sensitive and secretive nature. The secretive nature of these organisations prevents intelligence services from readily revealing their technological capabilities.

In this study, the technology issues are adopted from UTAUT variables that include *perceived expectancy, perceived simplicity and perceived compatibility*. The speed, acceptance, adoption and usage of SOCMINT in developed countries has increased as opposed to developing countries like South Africa (Stegen, 2019). The South African intelligence is still trapped in the one-dimensional cold war paradigm where threats are primarily seen as being of a military type (Lahneman, 2010). The country has not fully recognised or embraced SOCMINT as a new technology for intelligence gathering and it was evident during the July 2021 civil unrest (Stegen, 2019). The study will attempt to identify factors or vulnerabilities that have hindered

the utilisation of SOCMINT by South African intelligence organisations, reasons for the existence of the challenges or vulnerabilities. The study attempts to investigate the following or provide research evidence:

2.13.1.1 The intelligence community did not believe that utilising SOCMINT would improve their performance in identifying threats of national security.

2.13.1.2 The new intelligence collection discipline like SOCMINT was probably difficult to use because intelligence agencies mostly rely on covert operations to execute their mandate.

2.13.1.3 Important others (bosses, peers, subordinates etc.) in the intelligence community did not perceive SOCMINT as a valuable tool to adopt and use during the July 2021 unrest.

2.13.1.4 The intelligence community did not have the necessary expertise, skill and technology necessary to use SOCMINT. In addition, South Africa does not have the legislative framework or regulation that govern the use of SOCMINT.

2.13.2 Organisation Factors

In IS studies, the organisational context focuses on descriptive measures, which include, among other things, resource availability and skill in use, social influence, information sources and communication channels, culture, communication processes managerial beliefs and degree of centralisation, organisational size and scope (Eze et al., 2013; Kannabiran & Dharmalingam, 2012). For this study, we looked at top management support, poor communication and managerial beliefs and skills in use for intelligence gathering.

The direction of an organisation is influenced by the unique prerogatives of top management (Shiau et al., 2009). Evidence suggests that top management creates an environment that is supportive and communicates and reinforces organisational principles through a clear vision, making them one of the most important factors in the adoption of new technology. The successful SOCMINT adoption in the intelligence community is influenced by top management, as they make decision concerning the adoption and future adoption of any new technology. The availability of all resources needed to implement SOCMINT is influenced by top management (Dahnil et al., 2014). Managers that stay current with evolving technology and have a positive attitude toward the deployment of SOCMINT can promote its advances

(Tarafdar & Vaidya, 2006). To accommodate SOCMINT, new structures with social media and technical skills are imperative. For the intelligence community to remain relevant in the information age and remain the provider of choice, it will have to outsource capabilities not available within the organisation.

Poor communication processes are cited as contributing to project failure. The lack of information sharing between the various intelligence communities has hampered the efficient use of technological collection methods, which has a negative impact on national security (Copeland, 2004 and Jervis 2006). According to Lowenthal & Clark (2015), the internal competition between various intelligence communities in a nation has an impact on the obstacles to information sharing, which affects its effective utilisation. The civil turmoil in South Africa in 2021 made this issue clear.

2.13.3 Environmental issues

The Intelligence community has unique characteristics in terms of organisational structure. It includes state and national government and its exercise of power, norms, and culture, are distinctive. Currently, the following intelligence communities exist in South Africa, State Security Agency (SSA), Crime Intelligence (SAPS), Defence Intelligence (SANDF), National Communication Centre (responsible for co-ordinating and integrating foreign government signals and communication), Financial Intelligence Centre and National Intelligence Co-ordinating Committee (NICOC). These institutions currently use interception signals and there has been increased use of open-source information (Mostert, 2017). The mandate of these intelligence communities' emphasis the use of intelligence for the purpose of national security threat responses within the context of state and human security paradigms. In doing so, the elements of policy and regulation, political influence, legal framework, citizen influence, ICT infrastructure and higher authority support are some of the driving factors for environmental issues.

Omand, Bartlett, and Miller (2012) argue that SOCMINT needs an ethical framework considering the public authorities' rising interest in the data found on social media sites. The framework they provide calls for "integrity of motive," "sufficient sustainable cause", "authority", "proportionality and necessity", "informed consent", and "last resort". These guidelines could possibly be helpful when addressing the SOCMINT's ethics because they are a little vague (Bartlett & Reynolds, 2015).

2.13.4 Individual Factors

An individual dimension portrays the behaviours of employees within the organisation who will adopt the technology (Ahmadi, 2017; Wisdom et al., 2014). This includes personnel knowledge, skill, experience, innovation culture attitude and technology mastering. From an individual perspective, personnel skills are a significant factor in deciding whether to adopt IT innovation. IT and analytical skills i.e., data mining and predictive analytics are some of the methods presented by Bartlett and Miller (2015), that reshapes how SOCMINT is gathered, stored and processed. If an organisation that does not have the required skills to adopt SOCMINT as an intelligence collection discipline, it will be difficult for it to adopt SOCMINT even if there is pressure or expectations to do so.

The level of knowledge and skills one has regarding the use of a particular technology determines one's attitude towards that technology. Early users of new technology typically have higher educational levels (Rogers, 1995). According to Momami (2020), older persons lack the necessary experience to effectively utilise the internet and related technologies (social media), it is likely that they worry about own ability to learn how to use the internet. According to Aspasia and Ourania (2014) and Wamba and Carter (2014), managers' educational background significantly affects their use of social media technologies. Gong (2012), on the other hand, found no connection between education level and attitudes toward using social networking sites. The SOCMINT discipline was only coined in 2012, thus the older officials in the intelligence community might not have the drive to learn how to use social media as an intelligence gathering tool.

Since IS advances are extremely distinct technologies, no single proposed adoption model can account for all of their requirements. Adoption occurs only after a number of factors, including those that ordinarily seem advantageous, have been thoroughly considered. The TOE framework's theoretical strengths are therefore strengthened in this research by merging its contexts with UTAUT framework. The paper contributes to the theoretical and methodological conversation in the IS domain by conceptualising the research framework that combines TOE taxonomies with individual-related aspects of UTAUT.

2.14 Integrated TOE and UTAUT Framework

Literature has proven that intelligence collection disciplines like SOCMINT are essential tools in enhancing the mandate of the intelligence community. Therefore, it is crucial to understand the determinants of SOCMINT adoption and the framework that has risen to address IT adoption. According to Oliveira and Martins (2011), in order to comprehend the complex process of technological innovation adoption, it is crucial to employ an integrated theoretical model or framework. In this regard, the variables that are significant from an organisational and individual perspective needed to be considered for SOCMINT adoption. Likewise, human and organisational perspective are not covered by single-theory implementation. According to Rogers (1995), the prominent IT adoption framework are, the DIO and TOE. The two frameworks are frequently used to investigate the organisational perspective, while the UTAUT is frequently used to investigate the individual perspective on new technology acceptance (Caldag et al., 2019). Evwiekpaefe et al. (2018), emphasised that in order to achieve improved results, two or more theories must be joined, as integrated studies outperform single-theory studies.

In this study, the researcher explored the human perspective using the UTAUT framework while understanding organisational perspectives using the TOE. The primary rationale behind the inclusion of UTAUT in this analysis is its validation, yielding a 70% variance in usage intention, a significant improvement over the eight models that came before it (Venkatesh et al., 2003). Likewise, the selection of TOE as the primary rationale for the study is based on its strength, as this framework is already ingrained in the contextual environment of the theory (Haini et al., 2019). Consequently, it is the better alternative since it can predict the connection between intra-firm innovation and technology adoption in government agencies (Gibbs & Kraemer, 2004).

By creating the integrated TOE and UTAUT conceptual framework (Figure 4), this study sought to advance knowledge by examining the adoption of SOCMINT in the intelligence community. Different variables from the TOE and UTAUT were identified to better understand the adoption of SOCMINT in the intelligence community. Various researchers have used UTAUT and TOE framework for technology adoption: Investigation into OGD adoption (Lnenicka et al., 2022), Adoption of Cloud Computing (Khayer et al., 2020), Adopt Electronic Records Management System (Hawash et al., 2020) and Open Government Data (OGD) usage

in India (Sexena, 2016) have integrated UTAUT and TOE to understand the adoption of technology in government agencies.

2.15 Summary

This chapter reviewed literature on SOCMINT highlighting what SOCMINT is, as well as the opportunities and challenges of SOCMINT. Literature suggests that ineffective use of SOCMINT as an intelligence collection discipline has negatively impacted national security. SOCMINT ineffectiveness has resulted in numerous intelligence failures, for example Arab Spring, London 2011 riots and South Africa's July 2021 unrest. The greatest intelligence failures in history were attributed to the violence's surprise element and the intelligence's apparent inaction (O'Connell, 2005). This necessitates actions to channel knowledge, innovation methods and contributions of individuals or organisations throughout the world, to seriously pursue the trend toward real time data. It is important for the intelligence organisations in South Africa to institutionalise and operationalise SOCMINT in the intelligence framework. To achieve the institutionalisation and operationalisation of SOCMINT in the intelligence community, the TOE theory with the integration of UTAUT theory enabled studying the adoption on SOCMINT and the researcher was able to answer why the adoption of SOCMINT in the South African intelligence community relatively low, and what challenges are presented by SOCMINT.

CHAPTER 3: METHODOLOGY

3.1 INTRODUCTION

The research methodology shows how research study is conducted to answer the research questions. It also shows the research instruments used for the study. Leedy and Ormrod (2013), defines research methodology as procedures of identifying, collecting, processing, analysing information about a particular phenomenon. The research methodology for this study is adopted from Saunders et al. (2009). The present chapter covers several issues: First, it describes the research paradigm selected for this study, research approach and design for the study. The data collection techniques will be explained and the data analysis methods.

The research onion approach by Saunders et al. (2009), was found to be a suitable and an appropriate approach to conduct the study. As shown in Figure 5 below, the research onion presents research design elements such as philosophy approach, strategy, design, data collection and data analysis techniques and procedures (Saunders et al., 2009). Elements within the research onion were carefully 'peeled' to choose a suitable methodology for this study.

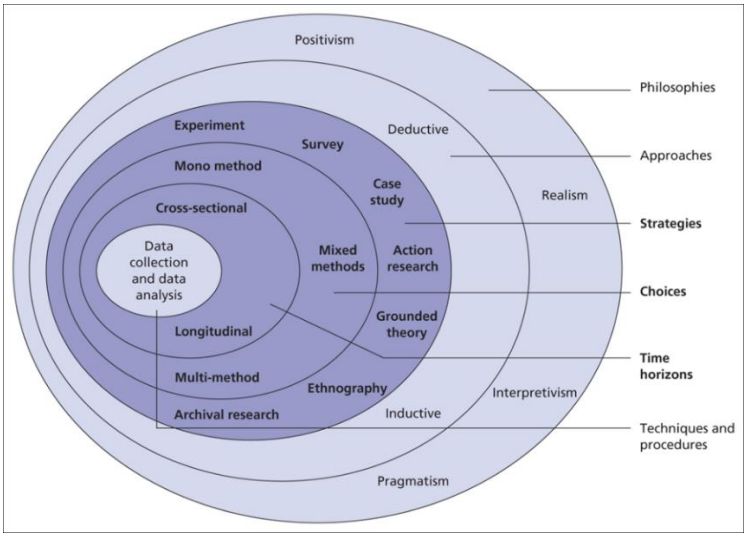


Figure 5. The research onion approach (Saunders et al., 2009)

3.2 Research paradigm and approach

According to Saunders et al. (2009), research philosophy is a set of presumptions and ideas about how knowledge is developed. There are four different philosophies in the research onion, Pragmatism, Interpretivism, Realism and Positivism. Pragmatism focuses on solving problems and it assesses truth in terms of effect, outcome, and practicality (Saunders et al., 2009).

Realism relates to scientific enquiry, and it emphasises that reality is independent to the human mind (Saunders et al., 2009). Jakobsen (2013), states that in positivism, knowledge can only be gained by objective, observable and measurable evidence. Interpretivism is based upon understanding the interpretations and meanings people give to actions (Dudovskiy, 2018). It is focused on how people interpret their own subjective reality. Therefore, this philosophy was found to be a suitable paradigm for this study. The major justification for this is that interpretivists use observation and interpretation of occurrences to understand social behaviour (Dudovskiy, 2018). This is done to comprehend social media's behaviour and its implication on intelligence and national security, because this study observes the social phenomenon of social media. The interpretive approach in this study offered an in-depth understanding of SOCMINT from the intelligence community's perspective, however their perspective was subjective based on their experience and knowledge. Officials from the intelligence community were in a better position to give their perspective and in-depth understanding on why the intelligence community is struggling to use SOCMINT as a tool to mitigate national intelligence threats. Thus, various versions of the truth and multiple conclusions were analysed and understood in diverse ways.

The research study was explored within the field of Information Systems (IS), specifically focusing on social media intelligence as an applied discipline. Due to the significant impacts from the three major disciplines of precise Technology, Sciences, and Social and Behavioural Sciences, IS has been referred to as an "inter-disciplinary" field. (Ahituv & Neumann, 1986). Oates (2009), states that interpretivism in Information System is concerned with the social environment of technology, the process by which IT is developed by people, and the subsequent process by which IT impacts people.

Distinctive characteristics of interpretivism are listed by Oates (2009):

3.2.1 Socially constructed meaning: social constructions creates and transfers reality in whatever form.

3.2.2 Researcher reflexivity: It is impossible to separate the researcher's background, including assumptions, views, and values, from the research, which inevitably affects the researcher's interpretations.

3.2.3 Multiple subjective realities: various versions of the truth can be understood in diverse ways.

3.2.4 Qualitative data analysis: interpretivism does not use the quantitative approach. Instead, the qualitative approach is much more suitable.

3.2.5 Multiple interpretation: multiple conclusions and interpretations are possible because the phenomenon can be explained in diverse ways by different researchers.

Saunders et al. (2011), describe two research approaches depending on whether the research is developing a new model/ theory (inductive) or testing existing new model/ theory (deductive). If one is interested in understanding why something is happening, it would be appropriate to undertake inductive research rather than a deductive study. Based on the research study, research objectives and research questions, the inductive approach was the adopted approach for this study because it is often used in social sciences research where the purpose is to understand the perceptions and behaviour of individuals (Saunders et al., 2009). According to Locke (2007), inductive approach involves moving from the specific to the general through empirical observation. Due to it connection to humanities and its subjective interpretation, inductive approach is informed by interpretivist philosophy.

3.3 Research Design and Strategy

The phenomenon under investigation was thoroughly analysed and socially explained by case study research using the interpretative research paradigm. Oates (2006), defines case study research as a thorough and focused assessment of a phenomenon in its natural setting with the goal of producing new information on the topic. To accomplish this, the intelligence community served as the only research case for the study because case study methods are helpful for analysing organisational behaviour, extracting cultural and behavioural knowledge, and identifying the tools, processes, and behaviours that have an impact on organisations daily (Yin, 2009). The case study is seen as singular opportunity, or perhaps even as a revelatory situation. This is because the researcher was able to investigate a subject pertaining to a sector with limited accessibility, which puts them in a unique position.

The following perspective are the guided principles for the case study:

3.3.1 Human perspective: the human perspective concentrated on human decision making within an organisation concerning the use of SOCMINT. This also included behaviours of employees within the organisation who will adopt the technology

3.3.2 IT perspective: this viewpoint focused on how SOCMINT is theoretically positioned inside an organisation. Focusing on the organisation's theoretical positioning of SOCMINT.

3.3.3 Organisation perspective focused on SOCMINT gaps and why the gaps continue to exist.

3.3.4 Environment perspective focused on the dynamics of the intelligence communities and the challenges that continue to exist.

This research study employed an exploratory case study methodology, which is a strong methodological choice for a field with little academic research but where data is readily available from personnel and national security agencies. Exploratory research is conducted when a problem is present but not well characterised (Du Plooy-Cilliers et al., 2014). It is also applied when something new is being investigated to become familiar with unknown situations or policies (Du Plooy-Cilliers et al., 2004). In this situation, the research's objective was to explore and investigate South African intelligence community's challenges and vulnerabilities in utilising SOCMINT as a tool to mitigate national intelligence threats as a result failing to predict or prevent the July 2021 unrest. The purpose was to increase knowledge that might one day be used by the intelligence community.

3.4 Case Study Approach

To address fundamental problems about SOCMINT adoption and use within the intelligence community, this study employed a qualitative case study approach. Oates (2006) defines case study research as a thorough and focused assessment of a phenomenon in its natural setting, to produce new information about the topic. Yin (2009), lists the characteristics of a case study, namely:

3.4.1 Investigates in detail a phenomenon within its natural surroundings. This study aimed to gain insight into challenges to the adoption of SOCMINT from the intelligence community.

3.4.2 There are no clearly defined boundaries between the phenomenon and its setting.

3.4.3 Existing theories were cited and used as guidelines for gathering and analysing data.

The intelligence community served as the only research case and the challenges of adopting SOCMINT as the only unit of analysis, the study used a single case design. The organisations' mandate include forewarning, predicting and developing operational plans that will inform government on any threat to national security. The case study is seen as an exceptional chance, or perhaps even as a revelatory instance (Yin, 2009). In a situation of having access to a wide range of resources within the case organisation, the researcher was in a unique position to investigate and explore a phenomenon related to a sector with restricted accessibility.

3.5 Time horizon

In research time horizon, there is longitudinal and cross-sectional studies. Longitudinal study makes observations on key characteristics of one group of people over an extended period (Saunders et al., 2009). This time horizon was not suitable for this study because the researcher needed to conduct the research in a brief period, and it can only take place in 2024. Hence the cross-sectional study was appropriate. Saunders et al. (2009), describes cross-sectional as studying a particular "phenomenon at a particular time". The advantage of cross-sectional is that it is quickly to do, and it is cost effective.

3.6 Data Collection Methods

Research data collection methods consist of primary and secondary data. The researcher believes in multiple realities to understand all perspective of the realities; hence the qualitative methodology was the chosen approach for this study. Several methods of data collecting, include interviews and field observations for primary data collection. Secondary data come from academic or scholarly journals, books and professional publications, scholar that have already been published (Myers, 2009).

Qualitative methods, such as interviews enabled the researcher to explore the perspective and views of those who have experience and use of SOCMINT as an intelligence collection discipline. Interviews are a form of a conversation between two or more people. The questions must be concise and unambiguous to be able to get a response from the interviewee (Saunders et al., 2009). The interviews were semi-structured in nature because they combined the components of both structured and unstructured interviews. According to Oates (2006), the purpose of semi-structured interviews is to encourage discussion toward the established study objectives while also providing chance for the information to naturally become known. Themes

and questions that the researcher addressed were on a list, however the questions and themes changed from interview to interview. This allowed the researcher the freedom to find and elaborate on information that the research might not have considered relevant but that participants felt was significant (Gill et al., 2008). To get a deeper understanding and provide the participants the opportunity to comment on their impressions and opinions, the interviews included open-ended questions linked to the study paradigm.

A sampling strategy was based on the non-random selection of Intelligence community (IC) experts and analysts. The focus of the study concentrated on individuals and experts who have knowledge of social media from a perspective of national security threat and intelligence specialists who have used SOCMINT for intelligence gathering. Therefore, Non-random selection is a kind of non-probability sampling. Babbie (2010), define sampling as a method of selecting a subset of people from a large population and that part of a group is to represent the entire population. Bless et al. (2006), identifies two types of sampling, namely non-probability, and probability. In probability sampling, there is a likelihood that any member of the population will be included in the study (Bless et al., 2006). Non-probability is snowball sampling, convenience sampling, purposive sampling, and quota sampling (Bless et al., 2006). This means subjective methods are used to select participants (Etikan, Musa and Alkassim, 2016).

The participants in the population were not all given equal chance of being included in the sample. To gain an organisation-wide perspective on the challenges of SOCMINT adoption, a variety of participants were interviewed. These included users (officials who use SOCMINT extensively), strategists (officials who use SOCMINT to build strategic models and products), and technical specialists (analysts) involved in the day-to-day operational design. The participants also included retired intelligence experts who have knowledge in intelligence gathering. These were retired intelligence officials who have made provocative extraordinarily valuable contribution to the understanding of intelligence gathering using SOCMINT. A purpose sampling was adopted for this study. Purposive sampling is adopted when the researcher selects who to interview (who to include in the sample) based on a set of traits (Du Plooy-Cilliers et al., 2014). The purposive sampling identified intelligence experts and retired intelligence officials. The snowball sampling was also employed to select other participants based on their role and area of specialisation within the organisations.

3.7 Data Analysis Method

Data analysis is defined as the process of giving a large volume of data order, structure, and relevance and to gain an enriched understanding of a phenomena, it involves sifting, sorting, selecting, and organising (De Vos, Strydom et al., 2011). For this study, a thematic analysis was the appropriate data analysis method. Thematic analysis emphasises pinpointing, examining and recording patterns or themes within data (Clarke & Braun, 2013). Smyth et al. (2012), states that in thematic analysis, data analysis codes are used to group sections of text with similar content into categories that can be combined for a final analysis. As coding progresses, memos were written to document emerging themes. A thematic analysis enabled the identification of patterns and themes within data (Clarke & Braun, 2013).

Table 4 Qualitative thematic analysis (Clarke & Braun, 2013)

Steps	Data Analysis Technique	Technique description
1	Familiarisation with data	Collected data from interviews was read and reread, audio recording collected from the interviews are listened and transcribed into text (words). This ensured that the researcher is intimately familiar with the data.
2	Coding	Interview transcripts were scrutinised to identify features of the data that relate to the research questions. Scrutiny was done to reduce data into smaller and more meaningful chunks. The researcher coded the features and meanings that were relevant to the research questions.
3	Searching for themes	Related codes were sorted into some sort of order or into groups to create meaningful data pattern (themes)
4	Reviewing themes	Extracted codes are related to the themes. The researcher checked to ensure the relation.
5	Defining and naming themes	The researcher wrote a detailed analysis of each theme.

6	Writing up	The analysis was transformed into interpretable piece of writing that relates to themes and research questions.

The following thematic analysis method was conducted:

3.7.1 Step 1: interview sessions were formally recorded and collected data from interviews, was SSread and audio recording collected was listened and transcribed into text (words). This ensured that the researcher was familiar with the data.

3.7.2 Step 2: The transcript for every given meeting was coded by the researcher. Coding was established and modified throughout the coding process. Early codes therefore demonstrated a mixture of already-established theoretical concepts and recently emerging concepts in the field.

3.7.3 Step 3: To create groupings of codes, relevant codes were gathered. The sorting of high-level categories helped to reduce the volume of data. The codes were modified in the coding process.

3.7.4 Step 4: The categories were named into themes for identification purpose. As the coding progress, the researcher identified a relationship within the categories. Emerging themes were based on the TOE framework together with the UTAUT framework.

3.7.5 Step 5: Identified themes were defined and discussed based on the findings. Each emergent theme was classified as either a challenge or non-challenge. Only the challenges were giving further consideration, in line with the purpose of this study to identify the challenges to SOCMINT adoption.

3.7.6 Step 6: The identified themes were interpreted by using a vivid and convincing extract example.

3.8 Ethical Consideration

There are particular and significant ethical, legal, and political considerations that are raised when human subjects are the focus of study (Tripathy, 2013). The first objective was to protect human participation. The researchers must not expose volunteers to danger (Louw, 2014). The interview was carefully compiled to remove any rude or discriminating comments (Resnik,

2011). The results of the research were used to benefit the intelligence community or society rather than just the person doing the study for personal gain. It is important to ensure that information is not falsified or misrepresented to favour a particular outcome or findings to produce results in the researcher's favour (Louw, 2014).

Due to a nature of the research, the following factors were considered:

3.8.1 Consent was required from the participants

3.8.2 Transparency and rights of participants

3.8.3 Participation in the study was voluntarily

3.8.4 Participants had the right to withdraw at any point without consequences

3.8.5 Anonymity of the participants and the confidentiality of the information will be kept

3.8.6 An ethical clearance was obtained from Wits University

3.8.7 A gatekeeper's letter from the intelligence organisations to interview their employees was obtained

The above factors mean that all participants participated in the study voluntarily, and their identity was kept confidential throughout the study. Their personal information or identity will not publish or disclosed to anyone. With the permission of the participants, the interviews were recorded for some participants using a smartphone. Others were uncomfortable due to the nature and the sensitively of their environment. All participants were required to sign a consent form which gave guidelines about the subject under investigation, however they were allowed to withdraw or refuse to participate at any point with no negative consequences. Additionally, a request for ethical clearance was made to the University of the Witwatersrand to perform the study and gather data from human subjects. The ethical clearance and the consent form are attached in Appendix A and E.

3.9 Summary

This chapter explains the methodology on how the study was conducted to answer the research questions. The interpretivist paradigm was selected for this study, this means that the understanding and interpretation of SOCMINT may be subjective to expert's reality. The chapter explains that qualitative research was conducted where the participants were

individuals and experts who know social media from a perspective of national security threat and intelligence specialists who have used/ are using SOCMINT for intelligence gathering were interviewed on a one-on-one basis. The participants also included retired officials who have made provocative extraordinarily valuable contribution to the understanding of intelligence gathering. The chapter also described how data was coded for analysis. This is discussed in detail in the next chapter.

CHAPTER 4: DATA ANALYSIS AND FINDINGS

4.1 INTRODUCTION

This chapter reviews the case documentation and analyses gathered from twelve participants through interviews. This study used semi-structured interviews as a qualitative data collection approach and theme analysis to interpret the data, in keeping with the points made in Chapter 3. This chapter also addresses the findings and how they should be interpreted in light of the reviewed literature. The suggested conceptual frameworks were improved using the findings to incorporate important variables that were discovered throughout the investigation; the updated framework is offered in the summary section of this chapter.

4.2 Participants

Interviews were conducted in a semi-structured format with participants from the case organisations who were involved in SOCMINT adoption initiatives or decision-making processes, as well as those with experience using SOCMINT, to collect data. At the start of the data collection process, the researcher sent emails requesting permission to conduct the research and also prepared an internal memo to obtain approval. The purposive sampling was used to identify the participants. The snowball sampling was also employed to select other participants based on their roles and area of specialisation within the organisations. Out of the emails that were sent, the researcher received fifteen responses, and they were keen to participate in the study. However, three participants could no longer participate in the study due to the sensitivity of their environment.

Profiling the respondents' job roles within the organisations revealed that 50% worked in the core business, which comprise of collection (HUMINT, SIGINT, OSINT), analysis, counter intelligence (offensive and defensive), and covert action and support functions, 30% were employed in the IT department, 20% were management (strategic role) and 10% performed support functions, which promise of technical, human resource, financial and leadership support. The participants' roles within the organisation were also considered when creating their profiles. A profile of the participants was created based on how long they had worked for the organisation. With majority of 70%, these are participants with more than ten years of experience. A total of 30% of the participants had worked for the organisation for more than four and up to ten years.

In summary, the characteristics of the participants listed above indicate that the study's sample accurately represents the main actors involved in SOCMINT adoption. The majority of the sample's respondents had worked for the organisations for more than five years, which was consistent with the participants who were intended to be included—that is, individuals with the necessary experience informing and/or influencing SOCMINT adoption inside the organisations.

Table 5 The following participants were interviewed

Participants	**Job roles**	**Approximate Years in Org**
Participant 1	Support functions	>10
Participant 2	Core business and IT Department	>6..8
Participant 3	Core business and IT Department	>10
Participant 4	Core business	>10
Participant 5	Core business	>10
Participant 6	Management and Core business	>10
Participant 7	Management	>10 close to retirement
Participant 8	IT Department and Core business	>10
Participant 9	Support functions	>6…8
Participant 10	Management and Support functions	>10
Participant 11	IT Department	>4…6
Participant 12	Former Senior Manager (retired)	Retired

4.3 Interview Questions Profile and Response Rate

Appendix C shows the division of the semi-structured interview questions into three sections. Given that 20 of the study's 25 total questions focused on the main research issues, it is evident that there were sufficient questions to capture the participants' perspectives on the phenomenon of interest. Of the 25 questions, a total of 22 (91%) received a 100% response rate, meaning that each of the 12 participants was selected to respond. The researcher considered the 91% average response rate to be excellent overall.

The researcher observed that the majority of the questions, which related to the participants' experiences working for the intelligence community, were easily answered by the participants. Several participants chose not to respond (reluctant) to questions related to the technological context of SOCMINT adoption. This is because there is a traditional assumption that everything about the intelligence business should be in the shadow, particularly in terms of intelligence technology developments. The sensitive nature of the environment was a reason why there was resistance to sharing information. Participants were asked if they had any additional factors that were not included in the study (i.e. factors missing from the proposed integrated conceptual framework). Factors like the acquisition process and organisational culture were raised as additional factors that can be included in the proposed integrated conceptual framework.

4.4 Documents Reviewed

Participants in the interview process mentioned pertinent documentation, which the researcher reviewed and cross-checked against the participants' insights like the Rica Act which governs domestic communication signal interceptions, the General Intelligence Laws Amendment Bill Amendment Bill (GILAB) Act is a new bill amending the powers and mandate of South Africa's state intelligence services and the National Security Strategy that is meant to enhance cooperative governance with the security cluster). Each document was cited by the researcher about the participants and any pertinent questions. Every document was examined to ensure that it was pertinent to the participants' answers to the given questions.

4.5 Presentation and Findings

The key adoption themes that emerged from the data collected were categorised into the SOCMINT adoption contexts from the TOE theory, namely Technology, Organisation, and Environment. Additionally, the Individual factors were also incorporated determining the behaviours of individuals within an organisation. The participants were deemed and found to have the necessary experience, expertise, and knowledge in the Intelligence Community as well as the necessary background in the adoption of SOCMINT technology. Every participant had vast knowledge and understanding of intelligence gathering and the use of SOCMINT to mitigate potential national security threats. The participants also provided examples of their involvement, use, and decision-making for SOCMINT adoption within the intelligence community.

Most participants emphasized the importance of SOCMINT in the intelligence community, alluding that the adoption of SOCMINT as an intelligence collection discipline should have predated their employment. For example, Participant #3 said, *"…..the technology should have been tackled around 2010 when the technology was still new and some of the social media platforms were not known to the South African society. Due to a massively growing online community, it has become increasingly important to understand the role social media plays to national security."*

Participant #2 shared the same sentiments stating that "social media leads to a better understanding of various issues relating to social behaviour, therefore the intelligence agencies should have addressed the technological intelligence methods from the very early stages of social media".

In total, five themes were identified and derived from the data collected through interviews. Each theme was further sub divided into sub-themes, as illustrated in Table 6 below.

Table 6 Summary of Themes

Conceptual Framework	Themes	Source of the theme (Literature or Interview)
Adoption	Adoption Concerns	Interview
	Adoption Decision	Interview
	Adoption Views	Interview
	Adoption Issues	Interview
Technology	Compatibility	Interview & Literature
	Simplicity	Interview & Literature
	Expectancy	Interview
	Security	Interview & Literature
Organisation	Management Support	Interview
	Technology Inclination	Interview
	Cost	Interview
Environment	Silos	Interview
	Government Regulations	Interview & Literature
	Coordination	Interview

Individual	Skills Shortage	Interview
	Training and Exposure	Interview

The participants identified the following as the main insights related to the *Adoption* theme, some of which are connected to TOE and UTAUT elements in the following subsections:

4.5.1 Adoption Concerns

Eight of the participants alluded that SOCMINT could result in misinformation and disinformation. The spreading of false or inaccurate information where the facts are wrong. Information from social media can be false with the intention to mislead. Participant #1 indicated that "*false information that is gathered and analysed can mislead the intelligence approach."* Most participants mentioned that SOCMINT is capable of providing forewarning or strategic warning, however by itself, it is not so effective in providing imminent data threats. Participant #4 mentioned that "*SOOMINT can be useful in giving situational awareness in the aftermath of an incident, but the risks posed by false information and misinformation contradict most of its conceptual usefulness, and most of the intelligence communities might lack some of the necessary resources or requirements to operate a situational awareness capability effectively*." Participants also raised concerns about information security because social media platforms are public and available to both strangers and known contacts. They may pose a danger to information security. Participant #2 *"Online, people lose a great deal of their privacy*". Because of this transparency, cybercrime has increased, which has an impact on national security.

4.5.2 Adoption Decision

The adoption decision, according to two participants, is based on several variables, including whether SOCMINT technology aligns with the organisation's mandate or operational requirements (such as information security, intelligence relevance, intelligence priority, and regulatory compliance) amongst many factors. Participant #3 mentioned that: "*Decisions about policies should be informed and supported by intelligence organisations. Supporting decision-makers in their policy-making is one of intelligence's goals. Nonetheless, intelligence is frequently used by decision-makers to affirm decisions already made. Before the intelligence community can consider the adoption of SOCMINT, the South African government must first develop a national data policy that will govern the use of social media platforms in our country.*

This will enable the country to have access to the data on the social media platforms without necessarily consulting or requesting the platform owners." Participant #2 indicated that: "In China, *online platforms like Google and Twitter are blocked in their country. These services are provided by the Chinese providers, such as WeChat and Weibo. Chinese authorities have also had some success in restricting access to the virtual private networks."* Furthermore, Participant #2 highlighted that "*these are some of the things that need to be considered before deciding between SOCMINT adoption*."

4.5.3 Adoption Views

All the participants alluded to the July 2021 unrest as an eye opener for the intelligence community because it showed the impact of social media on national security. There is a general call for the government to reconsider its traditional way of thinkingand operationalise the gathering of intelligent intelligence from social media platforms. The adoption of SOCMINT is being urged by the fourth industrial revolution. Participant #1: alluded that "*There is a need to harness social media as an intelligence collection tool."*

4.5.4 Adoption Issues

Participant #6 mentioned that intelligence organisations do have mechanisms in place and systems in place to counter and prevent social media platforms from becoming weaponised. Participant #6 "*The State Security Agency was able to identify threats that were possessed through social media during the July unrest, and they were able to react by developing intelligence reports that were submitted to the relevant structures."* Participant #7 on the other hand indicated that: "*It is necessary for the intelligence community to take necessary steps in capacitating human personnel with the technological expertise and ability. It is public knowledge that the South African Police Service (SAPS) did not have the capacity and resources to meet the policing demands created by the unrest*." Another key challenge to SOCMINT adoption within the intelligence community includes the legislation that governs the use of SOCMINT by intelligence communities. Nine participants acknowledged that there is no legislation that governs the use of social media platforms for intelligence purposes. There are no clear guidelines in the South African legislation regarding the application of SOCMINT for domestic national security, however *"....the act that can be relevant and applied in this situation is the GILAB and RICA Act*" according to Participant #4.

In the next sub-sections, the researcher unpacks the other three themes concerning the research questions.

4.5.1 What are the primary obstacles to recognising SOCMINT as an official intelligence collection discipline within the intelligence community?

There are many key factors considered by the South African intelligence communities which were mentioned by participants in their responses to the questions posed by the researcher. Concerning the Technology, Organisation, and Environment Contexts, the importance of Security, Technology Inclination, Government Regulation, National Security threats, Coordination and Silo, Top Management Support, and Resources and Capacity were frequently mentioned by the participants.

4.5.1.1 Technology Context

Four major technological challenges were identified, these being: (1) Compatibility; (2) Simplicity; (3) Expectancy; and Security. Each is discussed below.

4.5.1.1.1 Compatibility

In the world of the growing proliferation of the 4IR technologies, three of the participants from the technological environment emphasised that for the adoption of SOCMINT as an intelligence collection discipline within the intelligence community, there is technology that is needed to meet different facets of the organisation's requirement. This is because information is considered intelligent if it is relevant, timely, and accurate for decision-making (O'Connell, 2005). It is important to consider whether the innovative technology will work with existing organisation systems and processes (Ray, 2016; Safari et al., 2015).

SOCMINT is the latest addition to the source database of intelligence organisations. However, participants #2 and #4 alluded that the intelligence communities did not initially incorporate SOCMINT as one of the intelligence collection disciplines because social media can both be viewed as a threat to and an opportunity for national security. Therefore, SOCMINT must align with the required organisation's standard operating procedures.

Participant #2 "*The intelligence community's ability to adjust to the new security threats in general, the technological revolution in particular will determine the direction of intelligence*

in the future. This is because a crucial challenge the intelligence community has to deal with is that the ICT revolution has increased the pool of intelligence."

Participant #4 stated that "*there are several social media platforms and the volume of posts prevents clever identification of threats. The quantity of content posted on these platforms creates a challenge in identifying threats."*

This challenge seemed to be a burning issue with operations as they are the main users of the data collected for national interest. Participant #6 "*the extent and scale of social media platforms and posts present opportunities for automated solutions to increase processing efficiency at the expense of accuracy. This may compromise data integrity."* Participant #7 *"I think that the only way to validate the integrity of the data is through human intelligence. This is because SOCMINT can never be used in isolation."*

Participant #10 also raised a concern that "*a number of the platforms and volume of posts can prevent adequate identification of threats."* According to Statista (2024), as of April 2024, there were 5.44 billion internet users worldwide. Of this total, 5.07 billion, or 62.6 percent of the world's population, were social media users (Statista, 2024). The enormous quantity of user content posted to these websites creates a challenge in identifying national security threats.

All participants indicated that inadequate comprehension of the context of a social media message can impede accurate threat identification and possibly result in misinterpretation. The understanding context challenge reduces SOCMINT's efficacy.

4.5.1.1.2 Simplicity

Participants highlighted that it is good to recognise the potential benefits presented by the adoption of SOCMINT, but the obstacle of language stands in the way of effective threat identification, making the use of SOCMINT difficult. "*To detect threats, a successful SOCMINT program needs to be able to interpret a wide variety of languages (Participant #2)."* Patel et al (2019), claim that to prevent misinterpretation problems, SOCMINT will require government entities to possess multilingualism and cultural sensitivity across 193 nations. Participant #1 "*Interpreting social media data can be challenging due to linguistic and cultural differences. Targeted individuals may communicate in codes which will be difficult and can*

frustrate accurate threat identification. I think that failing to understand social media post's context properly potentially led to incorrect understanding."

4.5.1.1.3 Expectancy

David et al (1992), define expectancy as the degree to which a person or organisation believes that using a particular system or technology would enhance their job. All participants acknowledged that SOCMINT can transform the intelligence collection tradecraft. However, Participants #6 and #7 indicated that SOCMINT technology cannot provide human emotions and perspective. Participant #6 stated, *"In situations where we cannot penetrate platforms like your WhatsApp groups, we use clandestine operations by recruiting one of the group members who are willing to provide information."* Participant #7 "*Technology can never outperform human ability. Our organisation still believes in the old ways of doing things hence they have taken long to invest in technology like SOCMINT."* Participant #8 indicated that the fusion of HUMINT and SOCMINT is possible by recognising that human assets can never be fully eliminated no matter how technology evolves.

Human Intelligence seems to play a role in encrypted platforms where technology may have restrictions. Encrypted platforms can also pose challenges in penetrating certain social media platforms. The participants revealed that open-source SOCMINT capability relies exclusively on the ability to access unencrypted social media data. Participant #5 "In s*ocial media platforms like WhatsApp and private messages communicated in other platforms like X and Facebook. The organisation will have to engage with the platform operators or owners to identify the instigators."*

Participant #9 "We have to rely on WhatsApp and Facebook owners to get encrypted messages."

According to the Human Rights Commission report (2024), during the July unrest, a lot of posts supported and encouraged violence and looting. Incitement and the majority of violent posts most likely happened on private messaging services like WhatsApp or Telegram. Thus, intelligence communities could not access private messages from private encrypted platforms, and they had to rely on international platform operators.

4.5.1.1.4 Security

Two factors of information security were raised by participants. The first factor involves information security and privacy about the targeted organisations or individuals. The second aspect involved information security factors that need to be considered by the intelligence communities. During the interviews, all twelve participants brought up information security as well as data privacy and protection as factors of concern when it comes to the adoption of SOCMINT. Six participants from core business mentioned that people have a desire to protect their "rights to privacy" but the general public must understand that intelligence communities may infringe these rights to privacy laws in cases where they can pose a threat to individuals or to national security. Participant #5 acknowledged that "*in the past, intelligence communities specifically the State Security Agency was accused of abusing state resources as a result of infringing the right to privacy*". There were allegations stating that intelligence communities were misusing the bulk interception of electronic signals to spy on senior members of the ruling African National Congress, the opposition, and the society at large. This raised concerns among the public and it eventually led to the South African Constitutional Court finding that there was no law authorising the practice of bulk surveillance and limiting its potential abuse.

The researcher noted that those who are reluctant to adopt SOCMINT will most probably raise concerns about data retention, sharing, and security. Thus, a successful SOCMINT adoption and capabilities must adequately address data management problems.

Participant #4 indicated that "*The criticisers of SOCMINT may argue that retaining social media data for long periods of time increases the risk of misinterpretation and reputational damage. There is a belief that bulk surveillance and data collection through social media platforms create additional threats to managing and keeping the data secure."*

Participant #5 stated that "*….the challenges of SOCMINT adoption in the intelligence community could be because of past speculations of misuse of state resources, abuse of power and fear of peer digital surveillance."*

A decision by the Constitutional Court establishes a standard for intelligence operations in the SOCMINT area and suggests that these activities should normally be reserved for extreme circumstances. The decision by an intelligence agency to listen in on phone conversations and use social media platforms like X, Telegram, and WhatsApp may raise issues from the

standpoint of the "right to privacy." These social media platforms are unlikely to be considered public domain or open-source intelligence (OSINT) due to their stringent password and encryption protection (informed consent measures).

In countering and mitigating the challenges of abuse of power, privacy, and data security, the President of South Africa approved the first draft of the General Intelligence Laws Amendment Bill Amendment Bill (GILAB). GILAB seeks to provide for the following (GILAB, 2024):

a. "*a restructure the intelligence services to provide an institutional architecture that enables effectiveness and efficiency by establishing the domestic intelligence agency and the foreign intelligence service;*
b. *remedy the defects in the functioning of the Signals Intelligence Capacity as confirmed by the Constitutional Court;*
c. *address the weaknesses identified through the Financial Action Task Force (FATF) process, including measures to combat money laundering and terrorist financing by empowering the national security structures to investigate and conduct security assessment if a person or institution is of national security interest;*
d. *Strengthen measures to regulate and coordinate the private security industry as part of a broader national security approach; and*
e. *put in place measures to regulate the conduct of former members of the service and others with access to intelligence information."*

Participant #8 and #9 indicated that their use of SOCMINT in their organisation has been exempted from acquiring their communication interception equipment. The participants respectively mentioned the following:

Participant #8 *"The Constitutional Court's ruling against communication interception and the concerns of privacy were never applicable to us because of the nature of our mandate. We have been exempted to acquire the necessary interception equipment as regulated by the RICA Act. The issues of privacy and security of information were never a factor to us."*

Participant #9 *"We have continued to use mass surveillance equipment to capture the phone numbers and geographic locations of hundreds of people. We use the technology called the Grabber to listen to conversations and intercept messages."*

According to Participant #9 *"A grabber is one of the devices we use because it is a gadget that can clone cell phones and intercept calls and SMS messages, turning a phone into a tracking and monitoring tool".*

Data revealed that the Constitutional Court's ruling against the communication interception and bulk surveillance was more applicable to SSA and not the other intelligence communities. While other communities continue to acquire and use interception devices for social media monitoring, bulk surveillance and interception remains a challenge for SSA.

The developing and acquiring of any technology to monitor social media activities will need advanced technological knowledge and skill. All the participants acknowledge that the South African Public Service at large has been lagging behind in the adoption of technology, especially digitalisation because of its social obligation to address the triple challenges of poverty, inequality, and unemployment. Thus, any adoption of any technology will require acquiring the technology and services from third-party entities. While this is the case, this poses a security challenge.

Participant #6 "*Because the information security issues are significant in the intelligence community, the organisations cannot sustain the risk of keeping intelligence products under the control of the service provider."*

Participant #7 indicated that "*In a situation where the intelligence community have to acquire social media technology, they would require external skill and expertise. This may pose a security risk and exposes their intelligence collection methods."*

Participant #10 stated that "…*involving external service providers in intelligence operations will definitely pose a threat to the security of the information*." Another danger that an organisation may face when handing over application administration to a third party is loss of control, according to Janssen and Joha (2011). Participant #3 "*information security and ownership are one of the challenges that led to us taking long to adopt SOCMINT. We may have control of the SOCMINT technology provided by a service provider, but we may not know who the service provider is partnering with. It could be a foreign intelligence agency for all we know."*

Data analysis revealed that cyberattacks fuelled by artificial intelligence have the potential to target platforms for data collecting and transmission, utilising sophisticated malware to gain access to, exploit, or delete vital information and intelligence. Thus, procurement and contracting practices may hinder the intelligence communities' ability to adapt technologies due to the sensitivity of the environment.

4.5.1.2 Organisational Context

Three major organisational challenges were identified, these being: (1) Management Support; (2) Technology Inclination, and (3) Cost. Each is discussed below.

4.5.1.2.1 Management Support

All participants agreed that management play a leading and an educator role in the adoption of SOCMINT in an organisation. Literature attested to the fact that senior management makes a significant contribution to the adoption of new technologies, and their support is essential for technology projects to succeed (Oliveira et al., 2019).

Participant #3: "*I think that the success and failures of an intelligence organisation will be dependent on the effectiveness of management and their support to new development."*

In unpacking the role support of management when it comes to the adoption of any new technology, the most common answer the researcher received when posing this question to many interviewees was the increasing politicisation of the intelligence and security community in general, over the past decade or more. The ANC's inability to distinguish between the role of the party and the government is a challenge for South African government institutions in general and civilian intelligence organisations in particular because it has an impact on departmental service delivery and policymaking (Van den Berg, 2018).

Participant #1 indicated that "I think the r*eason why management has been lax in committing to the investment of SOCMINT, is because the intelligence community do not want to be seen as over policing."* Participant #4 responded, "*One of the reasons why SOCMINT was not recognised as an intelligence collection discipline is because the politicisation of the environment resulted in a prolonged regulating of the social of media."*

Analysis of interview data linked politicisation to the low prioritisation and lack of focus on initiatives such as SOCMINT by the organisation. There was the general consensus that indecisive decision-making, insufficient attention to priorities and commitment to certain projects was as a result of frequent staff changes and acting appointments. Participant #1: "*…the lack of unwillingness to SOCMINT adoption was because of the unstable leadership within the organisation, which has created lack of outright inclination."* Participant #2: "*We find ourselves in an unstable environment due to frequent restructuring and leadership changes."* The lack of prioritisation of such initiatives can also be attributed to the historical background of the organisations, whereby organisations have been led by individuals who are often with an apartheid security background and are not inclined to technology.

4.5.1.2.2 Technology Inclination

Technological know-how, training and processes were mentioned by several participants who indicated that they are critical for any technology inclination. All participants stated that the July 2021 unrest was an awakening for the intelligence community. They acknowledged that the failure to identify and respond to the planned unrest and to successfully support stabilisation operations was caused by a lack of technological capabilities, excessive secrecy, and inadequate resources. As a reactive response to the unrest, Participant #4 stated that "*…a detailed customised training, ongoing upskilling, knowledge transfer by service providers, and learning from the private sector are few of the human resource interventions which can be used by the intelligence community for SOCMINT adoption inclination*".

Participant #2 and #4 respectively, elaborated on the measures implemented to guarantee technological preparedness as follows:

"*I think there is realisation and identified need for a digital transformation strategy, what that looks like, for me, it's how does that enable operations to succeed and deliver on their mandate. The strategy for me is for the IT department to educate operations about the advancement of technology and its needs in the intelligence community. This approach will lessen the fears of technology, and the awareness will bring about knowledge and eventual inclination to adoption."*

"In order for the organisation's personnel as a whole to be able to utilise SOCMINT efficiently or support it effectively as well, they must undergo thorough training as part of our digital transformation."

Participant #10 indicated that the organisation had the necessary funding and equipment, including advanced systems to monitor social media, even before the Unrest. However, the implementation of these technologies was hampered, by burdensome administration and bureaucratic roadblocks. Participant #4 attested to the fact that processes within the organisation are lethargic due to the bureaucratic processes and the "need to know" process.

4.5.1.2.3 Cost

There was a difference of opinions among the participants on the challenges presented by cost in the adoption of SOCMINT. Participants #5 and #10 indicated that the intelligence community was not exempt from the difficulties that many other organisations encounter due to the unstable economy and socio-economic conditions in South Africa. Participant #5 "*I believe that everyone is having difficulty and not performing as well as they would like to due to budgetary pressure. IT cannot just go and spend money on SOCMINT technology because even that portion of the budget that has been allocated for acquiring resources is not as big as they would like it to be."* Participant #10 on the other hand stated that *"Law enforcement officials frequently state that their primary issues are budgetary and resource limitations, but I beg to differ."*

Literature points to cost as being a challenge to the adoption of any new technology, but when questioned if the cost would be seen as a significant barrier to the organisation's adoption of SOCMINT, the contradictions came about from the views presented by Participants #1, #3 and #11. These participants stated that as long as the SOCMINT initiative could show to be beneficial to the organisation, it was not seen as a barrier. Participant #1 "*the cost of the implementation would be minimal as the organisation does not have to pay sources for information."* Participant #11 *"we don't have to spend money on vehicles to surveil people, technology like SOCMINT can be used to recruit sources and profile targeted individuals."*

4.5.1.3 Environment Context

Three major environmental challenges were identified, these being: (1) Silos; (2) Government Regulations; (3) and Coordination. Each is discussed below.

4.5.1.3.1 Silos

The security sector is comprised of the State Security Agency, Crime Intelligence and South African National Defence Force, and other security clusters. When evaluating the adoption of technology, an organisation may, therefore, investigate other organisations that are similar to their own and base its decision to adopt technology on the practices of those organisations (Trope, 2014). Ten participants indicated that ideally, the security sector to a certain extent, should mimic each other in terms of adopting SOCMINT technologies irrespective of their different mandates.

Participant #3 revealed that "*It is difficult to mimic each other when it comes to any adoption of any technology because of the absence of a coherent approach to national security. This is because our definitions and interpretation of national security differs and our response to a potential threat will also differ."*

Participant #10 *said that "our use of social media monitoring is different from other intelligence communities because our goal and purpose is for eventual prosecution. The SSA on the other hand may use social media to advise relevant structures."*

Participant #9 "*our interpretation of social media mobilisation during the July unrest was initially not interpreted as a national security threat. As a result, our response to the violent activities had limitations and was hindered by a lack of resources."*

The silo nature resulted from totally ignoring the statutory role of NICOC. The structure is meant to coordinate the intelligence community and its products. Participant #11 stated that "…*despite numerous evaluations, strategic retreats, and high-level talks amongst the various participants, the Intelligence Coordinator has struggled to accomplish the goals and purposes of intelligence coordination."* Participant #10 on the contrary "*our intelligence coordination meetings have improved since the July unrest, but there are continuous concerns by Defence Intelligence that NICOC was 'dominated' by the SSA."*

4.5.1.3.2 Government Regulations

All the participants attested to the fact that no regulation governs the use of SOCMINT in South Africa. Participant #4 indicated that "…*since we do not have a legislation that governs the use*

of SOCMINT, the RICA Act was passed to prevent mischief involving the interception of communication. Under RICA, the state would have had a general legal protection to carry out SIGINT and SOCMINT intelligence activities. This is because RICA was aimed to control the manner in which intelligence services conduct their operations. But because of the Constitution Court ruling, the communication centres like National Communication Centre were found wanting." Analysis revealed that the NCC couldn't bring July unrest forewarning because their capacity is supposed to focus exclusively on foreign signals intelligence

Participant # 8 and #9 highlighted that the Criminal Procedure Act gives them the authority gives them the authority to surveil individual's social media accounts with the approval of a judge. They stated that the constitutional court ruling against RICA was never applicable to their organisation. As a result, they have continued to monitor social media activities of relevance.

Participant #4 indicated that "*The RICA Act regulates an explicit communication surveillance called lawful interception. The organisation's primary facility for lawful interception is the Office for Interception Centres (OIC). But the OIC's standardised lawful interception and the NCC's bulk communications surveillance are very different from one another."*

Data revealed that, due to its targeted nature, OIC is usually employed to monitor or get information about a particular individual who is already under suspicion in a criminal investigation. However, intelligence services conduct bulk surveillance as part of an intelligence operation to detect suspicious keywords, key phrases, and communication patterns. If the two bills (GILAB and RICA Amendment bill) before parliament are passed, government will be able to secretly monitor every South African's phone call, private messaging, emails, and online browsing history under the guise of "national security". Participant #3 "*We still don't know how the Rica amendment bill and Gilab 2023 would affect internal regulation at the NCC."*

4.5.1.3.3 Coordination

The primary finding of every commission and inquiry that followed significant intelligence failures in Western democracies (the Iraqi non-existence of weapons of mass destruction, including 9/11) has been a lack of coordination between intelligence agencies (High review panel, 2018). However, the coordinating mechanisms have consistently gotten stronger as a

result of these discoveries. The issue of whether South Africa had to wait for a significant intelligence failure before addressing its own shortcomings in intelligence coordination. Participant #3 indicated that the "*Over the years, the Intelligence Coordinator has battled to accomplish the goals and objectives of intelligence coordination since the coordinated entities opposed the NICOC specified functions. The lack of coordination is also related to Defence's limited mandate to collect national intelligence internally in South Africa."*

It is believed that the lack of coordination and approach to the July unrest have self-evidently proven to be ineffective. Participant #10 "*it was a great mistake, and a lesson learned on our part but at the same time, we are rectifying those mistakes. The NICOC meetings have greatly improved since the July unrest incident*." While Participant #10 acknowledges the improvement in coordination, Participant #12 alluded that "*despite these improvement in coordination, evidence shows a critical turning point in the way the government is responding to the rise in polycrimes set against the multifaceted security crime architecture of South Africa*."

4.5.1.4 Individual Context

Two major individual challenges were identified, these being: (1) Skills shortage; and (2) Training and Exposure:

4.5.1.4.1 Skills Shortage

One of the main obstacles the organisation is facing in implementing SOCMINT, according to the interviewees, is the shortage of skills. This can be attributed to SOCMINT still being the latest intelligence collection discipline. It is believed that the analytics resource skill would be able to execute SOCMINT solutions if provided with adequate training and exposure. Participant #2 "*There are undoubtedly many intelligent people here, sometimes their wonderful capabilities go unnoticed*." Participant #3 believed that the shortage of SOCMINT skills was a problem that might be solved by providing the current data analysts with proper training.

Participant #4 believed that skill shortage was a challenge because "…*social media intelligence requires Data Science and predictive analytics knowledge which is rare skill."* It is believed that the challenges are not only confined to their environments or government. "*Instead, it is a skill that relatively few people in South Africa possess" (*Participant #4).

4.5.1.4.2 Training and Exposure

The majority of interviewees emphasised the importance of training and exposure to SOCMINT technology. An analysis showed that there is a direct correlation between exposure to sufficient training and a shortage of skills. It is possible that inadequate staff training was impeding the organisation's adoption of SOCMINT. According to Participant #4, the intelligence community now has the right attitude to implement and manage SOCMINT technology, but insufficient exposure and training was the reason for the limitation.

Participant #4 stated that*: "It is important to partner with other training institutes within government, such as the training entities in Crime Intelligence, Department of Defence, Department of International Relations and Corporation (DIRCO) Academy, the National School of Government and others. This will ensure correct career pathing, extensive knowledge and understanding of any new technology that will advance intelligence capabilities."*

4.5.1.5 Other Factors

Upon completion of their interviews, participants were asked to specify any other factors they thought should be included in the study that the researcher might have overlooked as challenges of adopting SOCMINT. The following additional factors were highlighted by participants as potential additions to the framework:

4.5.1.5.1 Organisational Culture

Five participants noted that the organisational culture is another factor that influences SOCMINT adoption. They indicated that many of the leadership and management in the intelligence community come from the liberation struggle background. As a result, many of the leaders are not technologically savvy creating a challenge to technological inclination. According to Anderson & Perrin (2017), the rates of technology adoption among older persons are still much lower than that of the overall adult population, which is 90% who frequently use the internet.

4.5.1.5.2 Acquisition Processes

Three participants raised the acquisition process as another factor that influences adoption. They emphasised that the acquiring, developing or purchasing of SOCMINT technology will require compliance with the Public Finance Management Act (PFMA) process.

"Participant #6 stated that "*...because we are a government entity, we must align ourselves with the PFMA process. However, the procurement processes are prolonged, and they frustrate goods and service delivery. The bureaucratic processes make it difficult for us to adopt SOCMINT because today a certain leader will sign certain processes but because of the continuous change in leadership, the next appointed leader may not be aligned to those processes and may not approve the initiative."*

Participant #10 indicated that since the government was still handling cases of corruption connected to COVID-19, the disturbance in the July unrest directly affected how they managed their priorities. "*Covid-19 projects took top priority and resources were therefore redirected."*

4.5.2 What factors impede the effective adoption of SOCMINT, and what challenges are encountered during its execution?

The main elements listed in Section 4.5.1 were found to be the main challenges to the adoption of SOCMINT by the intelligence community, based on the responses given by the participants. According to a study by Haag & Eckhardt (2014), TOE factors can either promote or impede the adoption of any technology. Several participants' experiences suggest that certain reasons call for caution and careful diligence and may also cause a delay in the decision to implement SOCMINT. The following sections provide examples of why SOCMINT implementation is hindered:

4.5.2.1 Technology Context

Various technological factors with the TOE-UTAUT integrated framework were identified as reasons why the SOCMINT implementation is hindered.

4.5.2.1.1 Compatibility

SOCMINT successes are few examples of how the discipline has progressed from theory to successful practice. Participants stated that SOCMINT has been found to add value to operational capabilities however, a favourable decision to adopt SOCMINT will result from the intelligence community's priorities, processes, skill and data integrity.

Participant #3: "*It is important for all information sources to be combined and reflected in the analysis capacity. The technology must support the organisational operations and the brightest*

minds who possess technological competency must be able to support the adoption of SOCMINT. In my view, this is possible if the organisation develops a technology task team under the leadership of the National Communication Centre (NCC) which will be responsible for coordination various stakeholders. The task team would be used to give the intelligence community access to digital technology possibilities (within legal bounds) that would facilitate intelligence gathering in response to the developing crisis."

Participant #4: "*SOCMINT solutions to intelligence gathering was assessed and evaluated and it is now found to be a valuable intelligence collection discipline. However, the development and procuring of such a solution must be able to integrate with our systems without compromising sensitive and confidential information. The reason why it took us so long to adopt SOCMINT is because any collection discipline should never compromise the operations and our technological capabilities."*

Participant #11 indicated that technology has the tendency of weakening defensive counterintelligence capabilities against foreign detection. Defensive actions meaning the ability to prevent the opposition from obtaining valuable intelligence. Foreign intelligence agencies may be able to identify and expose intelligence officials, even those working domestically, thanks to an ever-expanding "digital dust" of publicly available information, big data analytics, and targeted cyberattacks (Katz, 2020).

Data analysis revealed that there is excessive focus on secrecy in the intelligence community and is not counterbalanced with accountability and transparency. There seem to be concerns about cyberattacks, compromise of data integrity, and volume of social media posts, however, the challenges do not justify why SOCMINT implementations were hindered.

4.5.2.1.2 Simplicity

Language interpretation was identified as one of the challenges that did not seem to encourage the adoption of SOCMINT, and it did not seem to bring a positive decision to acquiring and implementing such a technology. Participant #4 indicated that "…*natural language processing technologies can be used to analyse social media post but the technology still needs human analysis to increase the accuracy to the information."*

Participants could not justify why SOCMINT adoption was hindered. The majority of the participants did not highlight language interpretation as a challenge. Participant #2 *"there are safeguards that can be integrated with any other systems or solutions that the organisation has in place".*

There seemed to be contradicting opinions on why SOCMINT adoption was hindered, therefore making language interpretation an unpersuasive reason.

4.5.2.1.3 Expectancy

Operational participants identified a variety of issues that call into question the efficacy of SOCMINT including reliance on HUMINT, scope and context of information, and encrypted platforms. While most of the participants acknowledge that the core mission of HUMINT, handling, spying, recruiting and collecting intelligence will endure for the longest time but emerging technology like SOCMINT could transform the whole intelligence process. Participant #9 stated that agents can be spotted, developed, recruited, and handled through social media platforms, however, adoption of SOCMINT can be a challenge because, hostile foreign intelligence services will probably use AI-augmented tools to target human intelligence officers in addition to putting technical platforms under constant threat by infiltrating, manipulating, and deteriorating collection.

Participant #4 "*..the reason why SOCMINT implementation has been hindered is because Artificial Intelligence cyberattacks may use sophisticated malware to access, exploit, or destroy important data and intelligence. They may also target platforms for communication and data collection. And as an organisation, we may not have the technological capacity to mitigate the risk."*

Participant #5 and #10 revealed that the intelligence community's ability to gather intelligence on a wide range of national security threats has already been strained by the increasing quantity and variety of information in the social media platforms; further strain may be caused by use of emerging technologies that directly target and undermine South Africa's intelligence gathering.

4.5.2.1.4 Security

The intelligence community's extensive schedule for research, development, testing, and evaluation reflects particular challenges it faces, and the security measures it must consider, but it also limits its ability to develop new technologies quickly and the speed of adopting new technology. Privacy and information security were raised as challenges of SOCMINT adoption. According to Benlian et al. (2009), lots of organisations worry that adopting new technology could result in security risks and possible compromises of their data and information.

Participants #4 and #10 respectively indicated the following about security and privacy as the reasons why SOCMINT was hindered,

"*When you consider the POPIA regulations, you can see how important information security is. Social media policies mention the need for due diligence and the importance of privacy, which is related to POPIA. Therefore, the decision to adopt SOCMINT will essentially come down to whether or not POPIA and the GILAB Act is considered."*

"The fact that people's personal information will be controlled by our law enforcement agencies will raise a lot of questions about security, including how safe these individuals are given the credibility of our organisations."

There are numerous acts of cyberattacks around the world, because collecting data using SOCMINT operations create an additional threat of managing and keeping the data secure. There is a risk because we might not have any control over the leakage of information (Katz, 2020).

There is a recognition that factors of information security or privacy should not hinder the adoption of SOCMINT because threats to national security can override concerns over personal information protection. Participant #3: "*If there is a need for us to protect the nation and its people, we will not consider any privacy or protection of personal information."*

4.5.2.2 Organisational Context

Three major organisational challenges to SOCMINT adoption were identified above and reasons for each challenge will be discussed below:

4.5.2.2.1 Management Support

There should be a clear distinct division of power, authority, and responsibilities between an intelligence service and those of the accountable political administration. However, this boundary seems to have been breached as expressed by the participants. Participant #1 indicated that the politicisation of the intelligence community was caused by Ministers and management interfering in operational issues "*interfering in operational issues mean interfering in processes and system that may enhance the collection discipline."* Participant #12 "*In most cases, Director Generals and Ministers do not have a good relationship, resulting in a negative impact on the collection and sharing of intelligence information*." Analysis revealed that political interference in operations or administrative processes undermines the notion of a professional intelligence service.

Another reason that was raised by the participants is South Africa's approach in appointing Director Generals or Heads of States. Participant #11 "*the appointment of the heads of service lies with the President and that makes them to be beholden to their appointers.*" This situation results in the politicisation of the agencies.

4.5.2.2.2 Technology Inclination

The failure of the majority of IS initiatives is frequently attributed to people and systems (Davenport et al. 2012). Participant #2 that the reasons for technological inclination challenges to the adoption of SOCMINT arise from unclear communication and lack of efficiency in processes "*the main issue that we have is the silos nature in distributing information in the organisation which makes the processes cumbersome."* The lack of distributing information can be directly linked to data integration. Inadequate integration of SOCMINT is said to impact end-to-end processing. Participant #12 highlighted that from an analyst perspective, "…*we have the collection, analysis, and processing office and they all use different systems. The problem is that the three systems need to talk to each other. That means that in order for these systems to interact and consume data, a large amount of data will need to be moved, transported, and exported into various locations."*

4.5.2.2.3 Cost

Participants revealed that cost management is one of the reasons why SOCMINT adoption is a challenge because operating costs are unpredictable and they include things like changing

resource use and growing expenses, which adds to the complexity of budgeting. For government organisations, cost management is important due to the PFMA regulations.

Participant #5 "*I'm not sure if the organisation is prepared for the financial and functional implications of SOCMINT due to many challenges facing the intelligence agencies. The country is still struggling to come to terms with the costs of the Covid-19 pandemic and considering the budget constraints by the national treasury."*

Participant #8 *"…before we can consider SOCMINT adoption, we need to ensure adequate training, resource and technology readiness because we don't want to end up with what Treasury call, fruitless and wasteful expenditure."*

Analysis revealed that due to the complex nature of the intelligence community, the audit process and approach are restricted to do the excessive secrecy of the operations. The covert operations prevent the community's annual audits from meeting the required standards, therefore not achieving an appropriate balance between secrecy and transparency.

4.5.2.3 Environment Context

Analysis revealed that external or environmental factors had an impact in the adoption of SOCMINT. This is because in the early stages of adoption, it is mainly coordination, consolation and legislation that would govern the use of SOCMINT.

4.5.2.3.1 Silos

The challenge of inconsistent information and interpretation is due to non-integration of operations, processes, and structures. Participant #11 "*The silo approach can lead to inefficiencies within the intelligence community. This is an important point to emphasise because the more we work in silos and fail to integrate operations and projects into various information centres, the more likely it is that we will fail or stumble in everything we attempt to do. Unfortunately, the consequence of this approach leads to intelligence failures as it was evident during the July 2021 unrest."* Participant #4 highlighted that the silos approach is caused by competitiveness within the community and leaders wanting individual glory.

4.5.2.3.2 Government Regulation

Five participants highlighted that controlling the internet in general and social media in particular is challenging. This is mostly due to governments' disagreements and lack of cooperation on matters like the agreement's governing body (Wu, 2015). In 2017, the Minister of the SSA called for a probe into social media regulation in response to the students and service delivery protest. The social media community in South Africa immediately responded to this by launching the #HandsOffSocialMedia movement, in which several community members voiced their displeasure with the idea of social media control (Van der Merwe, 2017). Participant #4 alluded that "*…the regulation initiatives were also met with reactions from the social media community."* Participant #5 *"...infringing on human rights will forever be an obstacle to the efforts of regulating social media."*

Participant #9 agreed that the main reason could be attributed to the way "*…we interpret the regulations because this may lead to its application and potentially infringe on human rights*." Participant #12 additionally brought attention to how a certain Act's interpretation prevented the organisation from using the data in its operations: "*The operation's interpretation of the Acts and their comprehension of my environment are the limitations*."

4.5.2.3.3 Coordination

The challenges of intelligence coordination have existed since the early years of democracy. Participants acknowledged that one of the reasons for this existing challenge is that NICOC is administratively and logistically at the centre of one intelligence service, the SSA. Participant #9 indicated that "*There was once a point when the then Minister wanted to put NICOC as a unit in his office*." Participant #3 attested saying that "*for the longest time, NICOC has been dominated by SSA, making the other communities resist its function*."

Participant #11 attributed the resistance and lack of coordination to power and competition, "*Intelligence communities are power dominant, which has led to increased competitive pressure as organisations strive to outshine each other*." However, a study by Thong (1999), suggests that the adoption of technology is not directly impacted by competitive pressure.

Participant #1 suggested that"*…there should be an independent entity that coordinates the intelligence services to avoid any dominances*." Participant #11 cited that "*the coordination*

challenges are not structural in the sense of where NICOC is located, but the challenges are more functional."

4.5.2.4 Individual Context

From an individual perspective, skill shortage and training and exposure are a significant factor in deciding whether to adopt IT innovation. The reasons for the identified challenges are presented below.

4.5.2.4.1 Skill Shortage

Most participants cited skills shortage as one of the major challenges faced by the intelligence community in adopting SOCMINT. Participant #10 "*It will be necessary to re-evaluate the skill sets of collectors and analysts in order to fully utilise and integrate SOCMINT and other technologies in the day-to-day collecting and processing of operations and workflows."* Participant #11 added that training and skills in SOCMINT "…*can only be eliminated if the human resource relocks their recruitment process*."

Participant 2# attributed the shortage of skilled SOCMINT personnel to the intelligence organisations not considering technology training and development to be a necessary component of the career pathing. Participant #9 indicated that "*The SAPS for example were not prepared to deal with the orchestrated July attacks because of insufficient training."*

4.5.2.4.2 Training and Exposure

Participants emphasised that inadequate training in law enforcement and intelligence agencies impedes prompt action and efficient crisis management. Participant #3 acknowledged that "…*financial limitations were having an impact on law enforcements, resulting in inadequately equipped intelligence organisations and an inability to assign an adequate number of personnel with training*."

Participant #12 attributed inadequate training to corruption and maladministration within the state security agencies "*funds are not directed or channelled to where they should go due to maladministration in government. And the maladministration is usually hidden under the cloud of covert operations*."

According to CSIS Intelligence and Technology Task Force (2020), adoption of technology may alter the resources available to analysts and collectors, but it may not alter organisational cultures or leadership perspectives of the training and abilities that should be given priority.

4.5.3 To what extent was information accessible to the intelligence services to adequately detect, comprehend, and respond to both the threat and the actual outbreak of the July 2021 unrest violence?

The study revealed gaps to the intelligence gathering and production obligations of the three intelligence communities (SSA, Crime Intelligence and Defence Intelligence). The participants revealed that even though the organisations have different mandates. It is therefore important to understand the extent of information available to the intelligence organisations to adequately detect, comprehend, and respond to both the threat and the actual outbreak of the July 2021 unrest.

4.5.3.1 Threat Identification

Participants alluded to the fact that the unrest was initially characterised by the arrest of former President Zuma where social media platforms (whether open and closed) were utilised to organise and aid in the spread of the unrest. However, the nature of the threat was not equally understood by the relevant parties.

Participant #6 stated that "*Threats to national, personal, and individual security were posed by the unrest, which either directly or indirectly endangered people's right to life and personal safety. However, the threat was not collectively understood by all intelligence communities."*

Participant #7 indicated that "…*South Africans are known to use violence as a weapon to express their displeasure. So, like the unrest, it was initially interpreted as another expression of displeasure. As a result, there was lack of response from the law enforcement."*

Participant #8 alluded that "*I believe that some of the behaviours were acts of terrorism and the National Prosecution Authority must prosecute some of the instigators on terrorism charges."* Participant #10 emphasised that *"…various aspects of the violence must be distinguished. There are those opportunistically took advantage of the situation but there are*

those who instigated the planning and violence through social media platforms meaning there were elements of terrorism."

There was a general consensus that while July unrest was characterised by social challenges and political challenges in the country, the violence was attributed to patterns of planning and coordinating public unrest, criminal activity, and protest. There is recognition that factors like political, economic, social and spatial were prevalent in the extent on which these played a role in the unrest.

4.5.3.2 Interpretation of national security threat

The study revealed that the security sector did not have a collective understanding of what national security threats are. There was an appeal by the Human Rights Commission for security sectors to urgently develop a National Security Strategy (Human Rights Commission, 2024).

Participant #3 "*It is important to have a collective national security strategy that will help corporative governance within the security sector."*

Participant #4 "I believe that the Defence Intelligence has a national security strategy that valid for five years. The document is available for public consumption, but I'm sure if the other intelligence agencies documents are available to the public."

Data analysis revealed that the definition of national security is vague and not clearly defined amongst the intelligence organisations, resulting in the lack of uniform approach to national security threats. According to Human Right Commission 2024 report, the Minister of SSA gave forewarning about the various widespread political and social unease. Participant #11 indicated that the "*the intelligence reports from the SSA were communicated to various intelligence structures, however there was lack of response from SAPS because their interpretation of national security threats was different from SSAs*." Participant #12 rearticulated the response saying that "*The early warnings were ignored and there was ineffectiveness in sharing intelligence report."*

4.5.3.4 Lack of Coordination

The participants were consistent in expression a lack of coordination among intelligence agencies and law enforcement. There was a consensus that for the longest time, the intelligence agencies have been working in silos. The consequences of the silos approach resulted in the July 2021 unrest.

Participant #6 stated that numerous joint security structures like NICOC were established to coordinate and provide intelligence assessments to the government by collating the information from all the intelligence services as well as other government departments. Participant #6 alluded that "*lack of coordination and information is one of the reasons why there was failure to response."*

Participant #10 mentioned that NICOC is meant to serve as the primary point of contact for clients who require access to intelligence and the agencies that gather it, guaranteeing that all available sources are incorporated into the intelligence picture and that the assessment product is processed and evaluated efficiently. "*The challenges of intelligence coordination in South Africa have been with the country since the early days of democracy*."

4.5.3.4 Social Media Understanding

According to the Human Rights Commission report (2024), social media platforms were used to strategically spread misinformation and disinformation, collaborative networks were formed and recruiting and mobilisation were established through various platforms (Human Rights Commission report, 2024). Closed platforms like Telegram and WhatsApp were used to instigate the violence. Weaponisation, videos, and pictures were shared through trending hashtags.

Participant #6 "*To be honest, early signs of mobilisation were presented in various social media platforms and the information was communicated to the relevant parties."*

Participant #7 "*As much as the signs of mobilisation were presented in different platforms, the quick spread of disinformation and misinformation was made possible by the speed and reach of information transmission on these platforms. It was therefore difficult to counter or mitigate the further fuelling of the unrest."*

Participant #9 also added that even though there were systems in place to collect data in an effort to prevent these platforms from being weaponised, the relevant parties either did not take action to advance their knowledge at the time or they lacked resources. "*While the one intelligence organisation identified the threats through social media, the other organisation did not speedy respond to the threats."*

4.5.3.5 Insufficient Capacity

Participants acknowledged that the intelligence agencies did not have the capacity to meet the policing demands. This could have been a result of financial constraints, training and other challenges within the organisations.

Participant #5 indicated that "*Unrest organisers appeared to have internal knowledge of intelligence agency's capability and resources, and they had purposefully chosen to target locations where the impact of a police presence would be minimal."*

Participant #6 stated "*The modus operandi of the unrest involved technology and rapid escalation, and it surpassed the capacity of public order policing."*

The researcher concludes that when choosing SOCMINT adoption, the intelligence community must consider several factors that pertain to Technology, Organisation, Environment, and Individual aspects. The above-mentioned concepts were brought up by participants. In most instances, security was seen as a critical challenge for technological adoption, and it needs to be considered and carefully evaluated before SOCMINT can be considered as an intelligence collection discipline. While Organisational and Environmental are the dominant factors for SOCMINT adoption, other factors like Organisational culture and Acquisition processes were seen as additional factors that may influence the adoption of technology. Overall, each key element identified by the participants corresponded with the factors found in the literature reviewed at the beginning of this study.

4.6 Summary

This chapter presented the researcher's findings from the twelve intelligence organisations' participants who were interviewed for the study. These results were analysed and applied to help formulate responses to the research's main and subsidiary questions. Lastly, the results were applied to improve the research's integrated conceptual framework. The study's accomplishment of the research objectives will be discussed in the upcoming chapter.

CHAPTER 5: DISCUSSION OF RESULTS

5. INTRODUCTION

The purpose of this section is to present findings about the research questions. The study aimed to investigate the challenges of adopting SOCMINT as an intelligence collection discipline. In order to investigate the research problem, research objectives were set and from the research objectives the research questions below were identified.

5.1 Discussion of findings

5.1.1 Why the adoption of SOCMINT is relatively low

Participants were asked to elaborate on why the adoption of SOCMINT was relatively low and the challenges presented by SOCMINT. The analysis of the data indicates that TOE together with the UTAUT framework were useful in framing the challenges of SOCMINT adoption in the intelligence community. The analysis revealed that the major challenges experienced were more organisational and environmental and less technological accept security as a factor of adoption. This might have something to do with the state of SOCMINT adoption in an organisation, where internal and external factors are typically the biggest obstacles in the early phases of adoption. TOE variables, as determined by content-based analysis by Haag & Eckhardt (2014), can either promote or impede the adoption of technology.

5.1.2 Technological context

All interviewed participants recognised, acknowledged, and accepted the opportunities that come with using SOCMINT to mitigate possible national security threats. Although the participants were able to give examples of different opportunities that could be derived from the adoption of SOCMINT, those from operations do not always recognise the value of SOCMINT. Participant #6 "*Since technology is unable to replicate human emotions and viewpoint, human intelligence continues to be the most significant and fundamental means of gathering intelligence."* Participant #7 emphasised that "*The operations of an intelligence agency must be conducted in secret to ensure the safety of the agency's operatives as well as the success of intelligence operations against threats. The best way to protect intelligence operations is still the use of human intelligence rather than technology."* The justification for not always recognising the value of SOCMINT emanates from the security concerns raised by those in the operations. Despite the preference for technical collection over human intelligence,

Wark (2003), argues that human intelligence will always play a part in the collecting process since some information, like perceptions, can only be obtained through human sources.

The concerns of security can hinder the decision to adopt SOCMINT due to the elements of secrecy surrounding the work of an intelligence service. Data revealed that with the necessary skills and expertise, SOCMINT technology should most likely be developed on-premises in case the intelligence community is unable to deploy all the security tools required to outsource. It is therefore possible for the intelligence community to vote against adopting SOCMINT technology if it lacks the necessary information security controls. According to Loukis et al. (2019), governance measures are essential for SOCMINT adoption without endangering the organisation.

Other technological factors or challenges raised by participants, compatibility, expectancy, and performance are unpersuasive and immaterial to the adoption of SOCMINT. Literature suggests the security experts' assessments, law enforcement agencies' successes, and usage of SOCMINT all offer evidence that the discipline can enhance the country's security.

Nevertheless, the participants' concerns demand intelligence communities' continued vigilance because any human-based system is fallible and needs continuous development to mitigate possible challenges.

5.1.3 Organisational Context

Data analysis with the interviewed participants uncovered a lack of technological inclination, organisational support, and cost as the major challenges to the adoption of SOCMINT. The adoption of new technology is unlikely to yield the expected gains if the viable resources and infrastructure required are unavailable in the government. Allen (2019), suggests that the major concern for South Africa is a lack of adequate resources such as IT infrastructure, skills, and digital technologies required for digital transformation. According to participants, the intelligence community had plans to initiate social media monitoring, but such initiatives were never financially supported. Senior officials' resistance to adopting change and digital transformation further exacerbated this. The study revealed that top management's inadequate financial planning for SOCMINT initiatives caused additional delays in the adoption of digital transformation. Participant #11 stated that "*our interest in internet and use of open-source intelligence collection started in 1996 after the dawn of democracy. But the initiative to further*

invest in the technology never materialised due to political interference and because we are led by individuals who are not technological savvy." According to literature, managers are unable to focus on employees, skills, and technological infrastructure when there is a lack of top-down leadership to guide digital transformation (Westerman et al. 2014). Participant #11 *"It is was not easy to discuss SOCMINT investment with the top management*." According to Yucel (2018), building IT infrastructure and acquiring resources are two ways to show that an organisation is prepared for digital transformation.

Integrating and utilising new digital technology is one of the obstacles organisations have when implementing digital transformation, according to literature (Van Dyk & Van Belle 2019). This can also be viewed as poor leadership and avoidance of SOCMINT organisational projects by top management. Inadequately informed leaders cannot advocate for what they do not believe in.

Data analysis also revealed that another key factor that led to the slowness in recognising SOCMINT as a relevant intelligence collection discipline, invariably, the most common answer received from many participants was the increasing politicisation of the intelligence and security community in general. Participant #1 "…*any intelligence organisations that serves the interest of individual politicians undermines the value of its intelligence products."* Participant #11 alluded that "*Political influence mean interfering with processes, and it weakens the integrity of an organisation. Politicians are afraid of an effective intelligence organisation and that is the reason why there was hesitant in investing technologies like SOCMINT."* Politicisation of security services or intelligence communities leads to divided loyalty (Expert High-Level Panel Report, 2018). When it comes to maintaining their political objectivity, intelligence agency personnel are faced with a dilemma when it comes to the possibility of violence stemming from internal conflicts within the ruling party. To safeguard national security, intelligence personnel must engage in operations that would target members of certain factions of the ruling party which would then expose them to accusations of political interference by individuals who may be monitoring them for illicit activities (Expert High-Level Panel Report, 2018). This creates an unwillingness to invest in technology that may be used for political policing. Participant #5, indicated that "…*the July unrest originated from within the ruling party's ranks, which raised questions about the politicisation of security services."*

5.1.4 Environmental Context

The Environmental context was identified as another challenge that hinders the adoption of SOCMINT as an intelligence collection discipline. These challenges include Silos, Government Regulations, and Coordination. Analysed data revealed that a collective approach to national security threats was not possible because a transparent National Security Strategy was not in place. If there is no clear National Security Strategy, there will not be priority and consensus in adopting SOCMINT as an intelligence collection discipline. Participant #3 "*there is an urgent need for the development of a National Security Strategy that will guide the country's understanding of national security and security threats because as far as I remember, the last approved national security strategy was in 2013. Things have evolved and technology has changed. In the early 2000s national threats were different from the 2024 intelligence threats.*" Participant #5 agreed that "*the existing security strategy is outdated because the possible threats which the country may have faced then is different to the threats we are facing today. Therefore, the systems and processes of countering threats should have evolved*." Literature also suggests that technological advancements have redefined the role of humans in the intelligence collection process and necessitated a response from intelligence communities due to their impact on national security (Katz, 2021).

Data analysis reveals that as long as there is no understanding of and approach to national security by the intelligence community, the need to redefine the intelligence collection methods and adoption of technology (SOCMINT) can never be a priority. The current existing National Security Strategy can never respond to the ever-growing digital and technological revolution. The nonexistence of a new National Security Strategy has a direct link to understanding national security threats. In a world of greater threat and greater transparency, technical capabilities are enhancing the intelligence community. As a result, intelligence communities can maintain their information edge through the disciplines of SOCMINT. This is because terrorist groups are a concern to national security since they use the same disciplines to recruit, organise events, and spread their ideology (Hamm & Spaaij, 2015; Jain & Vaidya, 2020). Additionally, social media mobilisation is another platform that has resulted in violence, property damage, and a threat to national security. Participant #4 indicated that "*…gathering intelligence using social media was never a thing. We only started to recognise the importance and the value of social media after the July unrest*." The slowness in gravitating towards the use of SOCMINT as an intelligence discipline could have led to one of South Africa's intelligence failures in history due to a lack of response by the intelligence and law enforcement

institutions in the July 2021 civil unrest. This meant that it was not impossible to swiftly respond to the early warnings of the unrest because social media was not recognised as a potential intelligence collection discipline. Another factor that could have gravitated to the slowness in recognising social media as a discipline, is the intelligence gathering and production obligations which the intelligence communities are respectively mandated to provide. Participant #1 "*The defence intelligence is not trained to deal with internal or domestic national security threats because of their limited mandate to collect national intelligence internally."* According to Section 2 (4) of the National Strategic Intelligence Act Section 2 (4), expressly prohibits the SANDF from secretly obtaining intelligence of a "non-military nature," except situations in which the President acting on the Minister of Defence's recommendation, uses the SANDF in conjunction with SAPS. Data Analysis reveals that the Defence Intelligence also could not have assisted in identifying national threats (July unrest) through social media intelligence because the threat was possibly not defined as military in nature.

Moreover, data also revealed that the challenges of SOCMINT adoption are also affected by the excessive secrecy in the intelligence gathering approach which eventually leads to a lack of coordination and a silos approach. Participant #5 "*The SAPS denied ever receiving the intelligence product from SSA while the SSA Minister insist on submitting the intelligence product to the relevant structured*." According to the July unrest Panel Review (2021), the National Police Commissioner did receive the intelligence reports before the Unrest, but the information did not specify the strategy or the specifics of how the Unrest would play out. There seems to be a breakdown in communication within the organisations and the security intelligence agencies. Due to the long-standing challenges within the intelligence community, operational intelligence collection methods failed to identify threats through social media and equally failed to respond to the unrest.

5.1.5 Individual Context

From an individual perspective, a shortage of skills and training are also significant factors in deciding whether to adopt IT innovation. IT and analytical skills like data science and predictive analytics were some of the methods that are necessary to reshape how SOCMINT is adopted. Analysis revealed that if an organisation does not have the required skills to adopt SOCMINT as an intelligence collection discipline, it will be difficult for it to adopt SOCMINT even if there is pressure or expectations to do so. Participant #2 highlighted that "…*as much we have some of the brilliant mind in the organisation, it is necessary to equip them with skills*

and knowledge that will us a technical advantage as an organisation." Participant #10 on the other hand indicated that "*Budget constraints are never an issue and should not be used as an excuse in implementing technology that will enhance our intelligence collection methods."* Data revealed that a shortage of skills and training and financial constraints are immaterial in influencing the adoption of SOCMINT.

5.2 Final Conceptual Framework for SOCMINT adoption

From the themes and sub-themes above, a new theoretical model for the intelligence community's decision to adopt SOCMINT as an intelligence collection discipline has emerged Figure 6 below illustrates how the enabling factors are influencing the decision of adopting SOCMINT, and it is informed by the data analysed in this study.

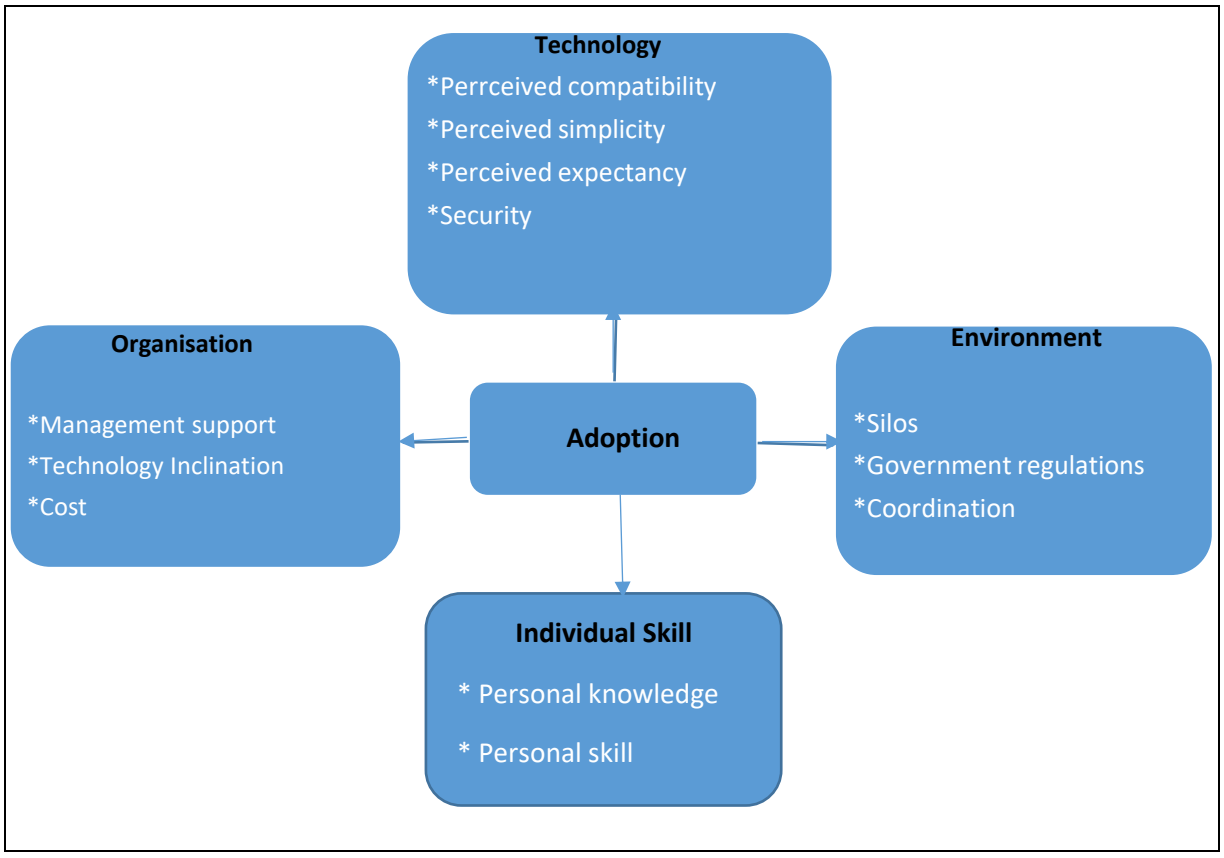


Figure 6 Final Intergraded Conceptual Framework

From the emerging theoretical model, the adoption factor is the central theme driving the implementation of SOCMINT. SOCMINT adoption concerns, decisions, views and issues are critical for technological, organisational, environmental and environmental factors.

5.2.1 Enabling factors to adoption centrality

The security theme is the single biggest ingredient in the technological factors that affects the adoption of SOCMINT. "*Emerging technology and artificial intelligence possess a security threat to the adoption of SOCMINT because it has the potential of targeting and degrading the intelligence collection methods and eventually weakening the intelligence community's capabilities*" (Participant #3). "*As much as technology like SOCMINT will transform the operating environment of the intelligence community, the intelligence officer will struggle to conduct covert operations because they run a risk of being exposed, or their agents, and their activities*" (Participant #5). It is there crucial for the intelligence to consider the security challenges that have a potential of weakening the defensive and offensive counterintelligence capabilities. The other technological factors (compatibility, expectancy and simplicity), participants indicated that social media volume and posts, context ambiguities, scope and scale, language challenges, encryption and data management issues are not too critical in the adoption of SOCMINT. However, because SOCMINT is a dynamic space in terms of how technology and threat impact policy the factors were retained in the conceptual framework.

Overall, for Organisation and Environmental factors, the majority of participants indicated that these factors as critical for SOCMINT adoption. Participants in the interviews emphasised the SOCMINT Characteristics aspect, which was included to the Organisational Environment Context.

5.3 Research questions addressed in this study

Social media is a relatively new field for intelligence collection in South Africa, and the nation has been sluggish to acknowledge the benefits of SOCMINT (Stegen, 2019). Since the beginning of democracy, one of the nation's intelligence failings has been the delayed recognition or implementation of SOCMINT as an intelligence gathering discipline. Violent civil unrest erupted in portions of KwaZulu Natal and Gauteng in July 2021. Among other instances, looting and economic harm were caused by social media mobilization during the disturbance (Civil unrest report, 2021). According to the expert panel's analysis of the July 2021 civil unrest, social media and open-source software were primarily to blame for the

devastation (Civil unrest report, 2021). Therefore, conventional methods of gathering intelligence, such as human intelligence were irrelevant.

Research objectives were established in order to instigate the research problem, and the following research questions were derived from the objectives:

5.3.1 What are the primary obstacles to recognising SOCMINT as an official intelligence collection discipline within the intelligence community?

5.3.2 What factors impede the effective adoption of SOCMINT, and what challenges are encountered during its execution?

5.3.3 What extent of information was accessible to the intelligence services to adequately detect, comprehend, and respond to both the threat and the actual outbreak of the July 2021 unrest violence?

In an attempt to address the research questions and learn what academics have to say about SOCMINT, a literature review was conducted. However, the research questions in the context of South Africa could not be addressed in the literature. This prompted a more thorough investigation where qualitative research was carried out through data collection, leading to the conclusions reported in Chapter 4. The following were the conclusions drawn from the literature and the qualitative data collected:

SOCMINT is the latest intelligence collection discipline that was only conned by Omand et al. in 2001. Many of the developed countries began conducting SOCMINT research and development projects to test the discipline’s ability as an intelligence collection method. There was realisation that the discipline could be applied in their work especially in countering terrorism (Kubovich, 2016). Social media is also used by South Africa's intelligence services to gather data according to their different mandates. The South Africa Defence Intelligence uses social media and the information to assist with planning, defending, and protecting the country. The Crime Intelligence on the other hand use social media to investigate crime and SSA utilise social media to identify possible risks, as well as to enhance their policies and gain a better understanding of current threats.

This research has often stated that the South African intelligence community has not completely adopted SOCMINT modern technologies to gather intelligence discipline resulting in one of the country's intelligence failures in history, the July 2021 civil unrest. The in-depth case study conducted offers some insight as to why, despite the opportunity presented, SOCMINT adoption is still in its infancy in the South African intelligence community.

Data collected and analysed revealed that the intelligence community could have avoided the July 2021 unrest if it had better technological collection networks and better cultural understanding of the targets and national security threats. Using the July unrest case as an example, the incident called for an organisational change as well as significant new technical collection initiatives that would have allowed various analysts from the community to exchange and access data gathered by other organisations. Analysis also revealed that relevant law enforcement structures received reporting on mounting protests, but the policymakers and institutions responsible for responding were not sufficiently alarmed by the reporting to take notice. The results emphasize many challenges that have hindered the adoption of SOCMINT as an intelligence collection discipline.

The study revealed the following about the adoption of SOCMINT by the intelligence community in conjunction with the research questions:

5.3.1 Absence of Legislative Framework

Legislative support for social media interception is lacking, which presents challenges for the SSA. The agency has the National Communication Centre (NCC) that is responsible for bulk surveillance however it is only applicable for foreign signal interceptions. Currently, no legislation governs the use of the centre (Swart, 2011). The amendment of the GILAB Act and the Rica Act shut off the holes that permit widespread spying.

5.3.2 Politicisation of the Intelligence Agencies

Findings revealed that the ruling party's inability to distinguish between the functions of the government and the party is currently a problem for South African government institutions in general and civilian intelligence organisations in particular. As a result, this has had an impact on departmental service delivery and policymaking. The situation led to the appointment of the high panel review with the main objective of realigning of the agency in accordance with the constitution and to ensure a responsible and an accountable intelligence agency. According to

Van den Berg (2018), the ANC's incapacity to distinguish between the role of the government and the party is currently affecting the policy-making process and departmental service delivery in South African government institutions generally and civilian intelligence organisations specifically.

5.3.3 Unstructured utilisation of SOCMINT

Findings revealed that the unstructured utilisation of SOCMINT is as a result of a vague understanding and interpretation of national security threats which are not clearly defined amongst the intelligence organisations, resulting in the lack of uniform approach to national security threats. This is because there was no prioritisation and effective coordination of the National Security Strategy. In June 2007, the first National Security Strategy (NSS) reached the Directors-General of the National Security Council (NSC), where it reportedly halted. Cabinet adopted the second NSS on December 4, 2013 (Daniels, 2019). The 2013 NSS is classified as Top Secret as is not accessible to the public including the security sector (High-Level Review Panel, 2018). The 2013 NSS was also deemed to be a business strategy that was too time-bound for the era in which it was created. Additionally, it makes very vague and unambitious suggestions for the architecture of national security (High-Level Review Panel, 2018).

5.3.4 Insufficient expertise and technological challenges

The change in the global technological environment requires new expertise and technical skills. Technical skills like data science and predictive analytics knowledge represent an impediment in the adoption of SOCMINT. The findings have highlighted that the challenges faced by intelligence organisations, particularly in South Africa, are not significantly different from those faced by other government departments. However, a key finding is that organisational challenges are perceived as greater hindrances than technological ones. Gower (2018), claims that just 29% of students enrolled in the majority of South African higher education institutions are in the fields of science, engineering, and technology. This falls well short of other BRICS nations like Brazil (33.9%) and India (42.6%). Therefore, this calls for innovative approaches that facilitate the adoption of SOCMINT by transferring digital literacy and skills between individuals and public officials.

5.3.5 Excessive application of secrecy

The findings have revealed that there is a lack of balance between secrecy and transparency which is directly linked to the silo's nature of the intelligence organisation and it has hindered effective accountability. Due to secrecy, intelligence organizations were immune to criticism before to 9/11, particularly during the Cold War era (Omand & Phythian, 2012). However, a balance between openness and confidentiality is required. The idea of "the balance between secrecy and transparency" is also emphasized in the South African White Paper on Intelligence (1995).

5.4.6 Security and Privacy

The public sector in South Africa has been slow to adopt technology, particularly digitalisation, due to its social responsibility to address the triple crises of unemployment, inequality, and poverty. As a result, to embrace any technology, intelligence communities will need to acquire the necessary services and technology from external parties, therefore posing a threat to national security. Cyberattacks fuelled by artificial intelligence have the potential to target platforms for data collecting and to gain access to, exploit, or delete vital information and intelligence. Social networking sites pose a serious risk to information security, according to Abdulhamid et al. (2011), since both strangers and familiar acquaintances can access them.
People's privacy is significantly compromised while they are online (Aronson & Cowhey, 2015). Cybercrime has increased as a result of this openness, which has consequences for national security.

5.5 Summary

Twelve intelligence experts made up the sample size for the study, which was carried out of the different intelligence community expects. Both IT and non-IT intelligence officials in different areas were interviewed. Given the problems and the cleavages in South Africa's society and the likelihood of the country experiencing outbursts of riots and looting, the research need was recognized in order to get insights into why the adoption of SOCMINT has been relatively low in identifying, forewarning and eventually responding to unrests or occurrences that may pose a threat to national security.

The key findings that stemmed from the study were the researcher developing an integrated theoretical framework which consists of Technology Organisation Environment (TOE) framework and UTAUT Theory. This integrated framework was used to investigate the

challenges that hinder the adoption of SOCMINT in the South African intelligence community. The research was able to identify organisational and environmental as the major factors of adoption. From the technological context there were no major challenges highlighted with the exception of security. Other technological factors or challenges raised by participants were unpersuasive and immaterial to the adoption of SOCMINT.

CHAPTER 6: CONCLUSION

6.1 INTRODUCTION

The study aimed to understand why the adoption of SOCMINT in the South African intelligence community is relatively low, and the challenges presented by SOCMINT. This was achieved by engaging in literature and gathering data through interviews with intelligence community officials who have experience and use of SOCMINT as an intelligence collection discipline. To conclude the study, this chapter presents the methods used to address the research questions. In addition, the chapter will also look at the challenges faced by the intelligence community in adopting SOCMINT as an intelligence collection discipline, the implications of the study, and present the recommendations.

6.2 Implications of this study

This study will provide valuable insights for the country's intelligence community since SOCMINT is a relatively new concept within the South African Government. The integrated TOE-UTAUT conceptual framework can potentially advance the Information Systems (IS) discipline, particularly when applied by academic researchers in the South African intelligence sector. To enhance intelligence collection methods and better identify national security threats, the study explores key Technology, Organisation, and Environmental factors in addition to individual and UTAUT factors that intelligence agencies must consider when deciding whether to adopt SOCMINT technologies. This framework may uncover new elements in future research that can help researchers understand SOCMINT adoption at the organisational level. The study also provides empirical data to inform decision-making regarding SOCMINT adoption and may assist in diagnosing the causes of any failures or challenges during the implementation phase.

6.3 Recommendations

The researcher made the following recommendations after completing the investigation, analysing the data from the findings, and reviewing relevant literature:

6.3.1 The July unrest demonstrated the importance of never taking the country's socio-economic and political conditions for granted and the need to continue monitoring this warning task on the radar even if the intelligence communities indicate other priorities.

6.3.2 Intelligence communities need to use new data-mining-based technologies to enhance their capacity to detect changes in sentiment shifts in the political and socio-economic spaces.

6.3.3 The Security cluster must urgently develop a national security strategy to promote intelligence priorities, coordination, and a clear and comprehensive definition of national security threats.

6.3.4 To counter the growing dangers of unrest, energy security, terrorism, and international organised crime, new approaches to recruitment, collecting, and analysis are required.

6.3.5 Budgetary constraints often prevent the intelligence community from keeping up with the most recent technological advancements. Through collaboration agreements, they can, nevertheless, benefit from innovation in the private sector.

6.3.6 Technological capabilities like artificial intelligence can be utilised to examine massive information to find patterns and anomalies in the form of deviations from patterns.

Maintaining continuity in leadership is crucial for inspiring the employees, implementing the new framework, and executing all of the new initiatives that are meant to enhance the intelligence priorities. The employment and use of SOCMINT may make it more difficult for people to trust the Intelligence Communities due to its intrusive nature. Omand et al. (2012), argue that SOCMINT needs an ethical framework in light of the public authority's rising interest in the data found on social media sites. They offer framework conditions, there must be a "good justification," "integrity plea," "regulative authority," "last resort," and "favourable outcome." These guidelines are not quite clear, thus they might be helpful when discussing SOCMINT's ethical issues. This might be a starting point for the South African intelligence community to develop a legislative framework to include social media surveillance as an intelligence collection discipline. This can be achieved by coordination with different governments and the public sector. To ensure that SOCMINT usage develops into an intelligence collection method in South Africa, users must understand the technological foundation, linguistics, and civil culture of society. Thus, there must be an effort to incorporate actors outside of the government, notably in the academic and private sectors. Developed nations like the United States (US) and Britain have improved intelligence gathering and analysis through the use of technological intelligence technology (Katz, 2020). Companies like Cisco and Nec, for instance, offer intelligence agencies in the United States a range of analytics

tools, including identity analytics, social media analytics, and video analytics (Hershkovitz, 2019). These platforms assist government organisations in employing real-time data stream analysis and machine learning to extract knowledge and generate predictions from previously acquired historical data using real-time data stream analysis (Hershkovitz, 2019). This could be a possible attempt to incorporate and apply SOCMINT within the South African intelligence environment.

6.4 Future Research

Even though this study developed a conceptual framework on the variables that influence the adoption of SOCMINT in the intelligence environment, several challenges still require analysis and investigation. Based on this exploratory study, future research can examine one or more of the major challenges in further detail, as well as how organisations address those issues. To further progress knowledge in the field of IS, future research should take into consideration improving the integrated TOE-UTAUT conceptual framework presented in this study. Similar studies might investigate other security clusters in South Africa or other countries. The results of this study might be tested quantitatively, such as by a survey, and a theoretical model could be created to better understand the challenges of SOCMINT adoption.

REFERENCES

Abramov, M. V., Azarov, A. A., & Filchenkov, A. A. (2014). What is more predictable insocial media: Election outcome or protest action? In *Proceedings of the 2014 Conference on Electronic Governance and Open Society: Challenges in Eurasia*. *Academic Medicine*. (EGOSE 2014), (pp. 157-161). ACM. http://doi.acm.org/10.1145/2729104.2729135

Abuhashesh, M. Y., Alamaireh, Q. N., Al-Dmour, H., Al-Dmour, M., R. E., Salman, A., R., & Boguszewicz Kreft, M. (2021). The role of social media in raising public health awareness during the pandemic COVID-19: An international comparative study. *Informatics*, 80, 1–19.

Aday, S., Farrel, H., Kelly, J., Lynch, M., Sides, J., & Zuckerman, E. (2010). *Blogs and bullets: New media contentious politics*. https://www.files.ethz.ch/isn/120788/pw65.pdf

Ahituv, N., & Neumann, S. (1986). *Principles of information systems for management* (2nd ed.). WM.C. Brown Publishers.

Ahmadi, H., Nilashi, M., Shahmoradi, L., & Ibrahim, O. (2017). Hospital information system adoption: Expert perspectives on an adoption framework for Malaysian public hospitals. *Computers in Human Behavior*, *67*, 161–189. https://doi.org/10.1016/j.chb.2016.10.023

Aid, M. M., & Wiebes, C. (2010). Introduction on the importance of signals intelligence in the Cold War. *Intelligence and National Security*, 25(3), 327–331. https://doi.org/10.1080/02684527.2010.489569

Akhgar, B., Bayerl, P. S., Sampson, F. & Switzerland, C. (2016). Osint as an integral part of the national security apparatus. *In Open-Source Intelligence Investigation: From Strategy to Implementation* (pp. 3–9). Springer.

Alkassim, R. S., & Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*. Musa, S.A. &, *5*(1), 1–4.

Allagui, I., & Johanne, K. (2011). The Arab Spring and the role of ICTs (feature article). *International Journal of Communications*, *5*, 1435–1442.

Allen, G., & Chan, T. (2017). Artificial intelligence and national security. *Intelligence and national security*. https://www.belfercenter.org/publication/artificial

Al-Menayes, J. J. (2015). Motivations for using social media: An exploratory factor analysis. *International Journal of Psychological Studies*, *7*(1), 43–50. https://doi.org/10.5539/ijps.v7n1p43

Ambinder, M. (2011). An intelligence failure in Egypt? *Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2011/02/an-intelligence-failure-inegypt/7082

Anderson, M., & Perrin, A. (2017). Technology use among seniors. Retrieved from https://www.pewresearch.org/internet/2017/05/17/technology-useamong-seniors

Ani, P. (2024). Worldwide digital population. Retrieved from https://www.statista.com/statistics/617136/digital-populationworldwide

Antonius, N., & Rich, L. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The International Technology Management Review*, *3*(1), 42–53. https://doi.org/10.2991/itmr.2013.3.1.4

Aspasia, V., & Ourania, N. (2014). Social media adoption and managers perceptions. *International Journal of Strategic Innovative Marketing*, *1*, 61–73. https://doi. https://doi.org/10.15556/IJSIM.01.02.001

Awa, H., Eze, S., Inyang, B., & Urieto, J. (2011). Upper echelon theory: A major determinant of information technology (IT) adoption by SMEs in Nigeria. *Journal of Systems and Information Technology*, *13*(2), 144–162.

Ayres, R. U., & Williams, E. (2004). The digital economy: Where do we stand? *Technological Forecasting and Social Change*, *71*(4), 315–339. https://doi.org/10.1016/j.techfore.2003.11.001

Babbie, E. R. (2010). *Introduction to social research*. Wadsworth Cengage Learning.

Bacastow, T. S., & Bellafiore, D. J. (2009). Redefining geospatial intelligence. *American Intelligence Journal*, 38–40.

Badiru, B. B., & Maloney, A. E. (2016). A conceptual framework for the application of systems approach to intelligence operations: Using HUMINT to augment SIGINT. *American Intelligence Journal Page* 41, *33*(2).

Baker, J. (2012). The technology–organization–environment framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), *Information systems theory* (pp. 231–245). Springer. https://doi.org/10.1007/978-1-4419-6108-2_12

Ball, D. (1989). Soviet signals. Intelligence (SIGINT*). Strategic and Defence Studies Centre*, Australian National University, 24–37.

Barbier, G. H., & Goolsby, R. (2011). Harnessing the crowdsourcing power of social media for disaster relief. *IEEE Intelligent Systems*, *26/3*, 10–14.

Barros, M. J. Z. D., & Lazarek, H. (2018). *A cyber safety model for schools in Mozambique*. Scitepress - Science and Technology Publications, (pp. 251–258). https://doi.org/10.5220/0006573802510258

Bartlett, J., & Miller, C. (2015). *The state of the art: A literature review of social media intelligence capabilities for counterterrorism*. Demos Publications.

Bartlett, J., & Reynolds, L. (2015). *The State of the Art 2015: A Literature Review of Social Media Intelligence Capabilities for Counter Terrorism*. Demos Publication. http://www.demos.co.uk/wpcontent/uploads/2015/09/State_of_the_Arts_2015.pdf

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. https://doi.org/10.1111/ips.12048

Bauman, Z., & Haugaard, M. (2008). Liquid modernity and power: A dialogue with zygmunt Bauman. *Journal of Power*, *1*(2), 111–130. https://doi.org/10.1080/17540290802227536

Bavelas, A. (1950). Communication patterns in task-oriented groups. *The Journal of the Acoustical Society of America*, *22*(6), 725–730. https://doi.org/10.1121/1.1906679

Benlian, A., Hess, T., & Buxmann, P. (2009). Drivers of SaaS-adoption – An empirical study of different application types. *Business and Information Systems Engineering*, *1*(5), 357–369. https://doi.org/10.1007/s12599-009-0068-x

Berger, J. M., & Morgan, J. (2015). *The ISIS Twitter Census (analysis paper)*. Brookings Institution.

Berkowitz, B. (2008). The R&D future of intelligence. *Issues in Science and Technology, Spring*, 37–46.

Bernard, R., Bowsher, G., & Sullivan, R. (2020). COVID-19 and the rise of participatory SIGINT: An examination of the rise in government. *Surveillance through mobile applications*. *American Journal of Public Health*, *110*(12), 1780–1785. https://doi.org/10.2105/AJPH.2020.305912

Bless, C., Higson-Smith, C., & Kagee, A. (2006). *Fundamentals of Social research methods', An African perspective* (4th ed.) p. 7780, Cape Town, South Africa, ISBN, 0702171948. Juta and Company Limited.

Böhm, I., & Lolagar, S. (2021). Open source intelligence: Introduction, legal, and ethical considerations. *International Cybersecurity Law Review*, *2*(2), 317–337. https://doi.org/10.1365/s43439-021-00042-7

Bonacich, P. (1987). Power and centrality: A family of measures. *American Journal of Sociology*, *92*(5), 1170–1182. https://doi.org/10.1086/228631

Borgatti, S. P., & Halgin, D. S. (2011). On network theory. *Organization Science*, *22*(5), 1168–1181. https://doi.org/10.1287/orsc.1100.0641

Breakey, J. (2017). Taking to the tweets: South Africa's relationship with protests and Twitter. Retrieved from https://memeburn.com/2017/02/south-africa-protests-twitter

Briggs, B. (2017). UK spy agencies share social media data with foreign governments, say critics. Retrieved from https://theferret.scot/uk-spy-agencies-share-social-media-data-foreign-governmentssay-critics

Burcher, M. (2020). *Social network analysis and law enforcement: Applications for intelligence analysis*. Springer Nature. https://doi.org/10.1007/978-3-030-47771-4

Burt, R. S. (1987). Social contagion and innovation: Cohesion versus structural equivalence. *American Journal of Sociology*, *92*(6), 1287–1335. https://doi.org/10.1086/228667

Byman, D. (2008). *The five front war: The better way to fight global jihad*. John Wiley & Sons, p. 24.

Byrne, B. P. (2015). They are shooting people one by one′ – Inside Paris concert hall. *Vocativ*. Retrieved August 5, 2022, http://www.vocativ.com/news/

Caldag, M. T., & E. G. (2019). Analyzing determinants of open government based technologies and applications adoption in the context of organizations. *International Conference on e-Learning, e-Business, Enterprise Information Systems, and e Government* (EEE 2019).

Chalk, P., Helmus, T. C., & York, E. (2013). *Promoting online voices for countering violent extremism*. Rand Corporation. http://www.rand.org/pubs/research_reports/RR130.html

Chao, C.-A., & Chandra, A. (2012). Impact of owner's knowledge of information technology (IT) on strategic alignment and IT adoption in US small firms. *Journal of Small Business and Enterprise Development, 19*(1), 114–131. https://doi. https://doi.org/10.1108/14626001211196433

Charani, S. (2016). Social Media's potential in intelligence collection. *American Intelligence, 33*(2).

Chen, H., Huang, S., Hung, Y., & Ku, C. (2008). Transplanting the best practice for implementation of an ERP system: A structured inductive study of an international company. *Journal of Computer Information Systems*, *44*(4), 101–110.

Chigudu, S. (2020). Rhodes Must Fall in Oxford: A critical testimony. *Critical African Studies*, *12*(3), 302–312. https://doi.org/10.1080/21681392.2020.1788401

Clark, R. M. (2020). *Geospatial intelligence origins and evolution*. Georgetown University Press.

Clarke, R. A., & Robert, K. K. (2010). *Cyber war: The next threat to national security and what to do about It.* HarperCollins.

Clarke, V., & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, *26*(2), 120–123.

Codruta, L. R., Ivan, I. A., Anamaria, I. C., & Nicolae, G. M. (2015). Social media intelligence: Opportunities and limitations. *CES Working Papers*. Centre for European Studies, Alexandru Ioan Cuza University of Iasi, *2015*, 506.

Copeland, T. E. (2010). *Intelligence failure theory, the international studies encyclopedia*, *15*.

Crosston, M., & Frank, V. (2017). *An intelligence Civil War: "HUMINT"*.

CSIS. (2020). *Intelligence and Technology Task Force research interview with U.S. intelligence organization*.

Dabhi, M. D. (2016). Geofencing: A generic approach to Real time location based tracking system. *International Journal of Computer Networks and Wireless Communications*, *6*(6/2016), 35–37.

Dahnil, M. I., Marzuki, K. M., Langgat, J., & Fabeil, N. F. (2014). Factors influencing SMEs adoption of social media marketing. *Procedia – Social and Behavioral Sciences*, *148*, 119–126. https://doi.org/10.1016/j.sbspro.2014.07.025

Daskevics, A., & Nikiforova, A. (2021). ShoBeVODSDT: Shodan and Binary Edge based vulnerable open data sources detection tool or what Internet of Things Search Engines know about you. *In Second International Conference on Intelligent Data Science Technologies and Applications (IDSTA*) (pp. 38–45). IEEE. https://doi.org/10.1109/IDSTA53674.2021.9660818

DataReportal. (2022). *Facebook Stats and Trends*.

DataReportal. (2023). *Facebook stats and trends.*

Davenport, T. H., Barth, P., & Bean, R. (2012). How "Big Data" is different. *MIT Sloan Management Review*, *54*(1), 22–24.

David, C., Gompert, H., & Binnendijk, B. L. (2004). *Blinders, blunders, and wars. What America and China can learn*. Rand Corporation [Ebook].

Davis, G. (2018). Bill to regulate online content approved. Retrieved from http://ewn.co.za/2018/03/06/billto-regulate-distribution-of-online-content-approved

Davis, J. (2023). *Libya's Arab Spring and Italy's post-uprising influence* (1st ed.) Imprint Routledge, *17,* eBook ISBN9781003378723.

DCAF (Democratic Control of Armed Forces). (2003). Intelligence practice and democratic oversight – A practitioners view. *Occasional Papers*, (3). https://www.dcaf.ch/sites/default/files/publications/documents/op03_intelligence-practice.pdf

Delport, C. S. L., De Vos, A., Fouche, C. B., & Strydom, H. (2011). *Research at grass roots* (4th ed.). Van Schaik.

Dover, R. (2020). SOCMINT: A shifting balance of opportunity. *Intelligence and National Security*, *35*(2), 216–232. https://doi.org/10.1080/02684527.2019.1694132

Du Plooy-Cilliers, F., Bezuidenhout, R., & Davis, C. (2014). *Research matters*. Juta and Company Limited, ISBN 978-1-48510-201-4.

Dudovskiy, J. (2016). Interpretivism (interpretivist) Research Philosophy – Research Methodology [Online]. *Research Methodology*. Retrieved from, http://research-methodology.net/researchphilosophy/interpretivism

Duffy, A., Freelon, D., Howard, P. N., Hussain, M., Mari, W., & Mozaid, M. (2011). Opening closed regimes. *What was the role of social media during the Arab Spring*. https://doi.org/10.2139/ssrn.2595096

Duijn, P. A. C., & Klerks, P. P. H. M. (2014). Social network analysis applied to criminal networks: Recent developments in Dutch law enforcement. *In A. J. Masys (Ed.), Networks and network analysis for Defence and security* (pp. 121–159). Springer. https://doi.org/10.1007/978-3-319-04147-6_6

Duncan, J. (2021). Data collection: ConCourt judgment on surveillance has far-reaching, global implications. *Daily maverick*. https://www.dailymaverick.co.za/article/2021-04-07-data-collection-concourt-judgment-on-surveillance-has-far-reaching-global-implications

Eaton, T. (2017). Internet activism and the Egyptian uprisings: Transforming online dissent into the offline world. *In Westminster Papers in Communication and Culture* M. Taki & L. Coretti (Eds.), *9*(2), 5–24). https://doi.org/10.16997/wpcc.163

Erwin, M. C. (2013). *Covert action: Legislative background and possible policy questions*. Congressional Research Service.

Evwiekpaefe, S. C., & Abraham, E. (2018). Individual and organizational acceptance of technology theories and models: Conceptual gap and possible solutions. *Pacific Journal of Science and Technology*, 189–197.

Eze, S. C., Awa, H. O., Okoye, J. C., Emecheta, B. C., & Anazodo, R. O. (2013). Determinant factors of information communication technology (ICT) adoption by government-owned universities in Nigeria: A qualitative approach. *Journal of Enterprise Information Management*, *26*(4), 427–443. https://doi.org/10.1108/JEIM-05-2013-0024

Forrester, B., & Hollander, K. D. (2016). The role of Social Media in the Intelligence Cycle. *Getting started—Tweepy*, 4.2.0 documentation. (n.d.). https://docs.tweepy.org/en/stable/getting_started.html#models

Fox, J. (2013). Intelligence analysis and the bureau: The evolution of analysis and the analyst position in the FBI, 1908–2013. *Journal of Strategic Security, 6*(3Suppl), 114–123. https://doi.org/10.5038/1944-0472.6.3S.12

Fund for Peace. (2023). *Failed States Index*. Retrieved from https://fragilestatesindex.org/

Ganesh, B., & Bright, J. (2020). Countering Extremists on Social Media: Challenges for Strategic Communication and content Moderation. *Policy and Internet, 12*(1), 6–19. http://library.wiley.com/doi/pdf/10.1002/poi3.236. https://doi.org/10.1002/poi3.236

Gause, F. G. (2011). Why Middle East Studies missed the Arab Spring: The myth of authoritarian stability. *Foreign Affairs, 90*(4), 81–90.

Genidy, A. S. H. (2018). The intelligence collection dilemma: How did overreliance on Techint produced intelligence failure? Case study*: The CIA failure in Iraq 2003, WMDs intelligence. Genidy_18731602_Dissertation-libre.pdf*

Gentry, J. A., & Gordon, J. S. (2019). *Strategic warning intelligence: History, challenges, and prospects*. Georgetown University Press. https://doi.org/10.2307/j.ctvb4bsfx

Gilbert, B. (2018). Facebook just published a message for its users: No, You're not the product. *Business Insider*. https://www.businessinsider.com/facebook-advertising-users-as-products

Gill, J., & Johnson, P. (2002). *Research methods for managers* (3rd ed.). Sage Publications.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal, 204*(6), 291–295. https://www.nature.com/articles/bdj.2008.192. https://doi.org/10.1038/bdj.2008.192

Golts, A. (2017). The Russian Army to be subordinated to the National Guard in a crisis. *Eurasia Daily Monitor, 14/76*.

Gompert, D. C., Binnendijk, H., & Lin, B. (2003). *The US invasion of Iraq*.

Gong, W. (2012). Factors influencing perceptions toward social networking websites in China. *In M. Strano, H. Hrachovec, F. Cudweeds & C. Ess (eds.), Cultural attitudes towards technology and communication 2012, proceedings of the 8th International CATaC Conference*, Aarhus, Denmark, June 18–20, pp. 420–429.

Goodwin, J. (2011). Why we were surprised (again) by the Arab Spring. *Swiss Political Science Review*, *17*(4), 452–456. https://as.nyu.edu/content/dam/nyuas/faculty/documents/Why_We_Were_Surprised_Again.pdf. https://doi.org/10.1111/j.1662-6370.2011.02045.x

Gutierrez, M. (2018). Maputopias: Cartographies of communication, coordination and action: The cases of Ushahidi and InfoAmazonia. *GeoJournal*, *84*(1), 101–120. https://doi.org/10.1007/s10708 -018-9853-8.

Haag, S., & Eckhardt, A. (2014). Organizational cloud service adoption: A scientometric and content-based literature analysis. *Journal of Business Economics*, *84*(3), 407–440. https://doi.org/10.1007/s11573-014-0716-6

Habib, A. (2019). *Rebels and rage: Reflecting on #FeesMustFall*. Jonathan Ball.

Haini, S. I., & N. Z. (2019). A conceptual model of open government data adoption for local authorities in Malaysia. *Open International Journal of Informatics (OIJI*), 7(1).

Halgin, D. S. (2012). An introduction to social network theory. Retrieved from http://jesuitnetworking.org/wpcontent/uploads/2013/10/halgin_social_network_theory.pdf

Hamm, C. (2012). Networks and national security: Dynamics, effectiveness and organisation. *Ashgate*.

Hamm, M., & Spaaij, R. (2015). Lone wolf terrorism in America. *Using knowledge of radicalization pathways to forge prevention strategies*, p. 9.

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction*, *31*(3), 498–501. https://doi.org/10.1093/humrep/dev334

Haneem, F., Kama, N., Ali, R. et al. (2017). Applying data analytics approach in systematic literature review: Master data management case study. *Frontiers in Artificial Intelligence and Applications*, *297*, 705–715.

Hawash, U. A. (2020). Intention to adopt electronic records management system in the Oil and Gas Sector in Yemen. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5).

Hayden, M. V. (2011). Egypt crisis doesn't reflect US intelligence failure. *CNN*. http://edition.cnn.com/2011/OPINION/02/08/hayden.egypt.intelligence

Hedley, J. H. (2005). Learning from intelligence failures. *International Journal of Intelligence and Counterintelligence*, *18*(3), 435–450. https://doi.org/10.1080/08850600590945416

Hegghammer, T. (2014) p. 1. *Interpersonal Trust on Jihadi Internet Forums*. Norwegian Defence Research Establishment.

Herman, M. (2009). Why should intelligence professional attend to intelligence ethics? *In 'A Symposium on Intelligence Ethics' Intelligence and National Security Special Addition*, 24(3), 366–386.

Hershkovitz, S. (2019). How tech is transforming the intelligence industry. *Google*. https://www.google.com/amp/s/techcrunch.com/2019/08/10/how-tech-is-transforming-the-intelligence-industry/amp/

HMICFRS (Her Majesty"s Inspectorate of Constabulary and Fire & Rescue Services). (2011). The rules of engagement: *A review of the August 2011 disorders*. Retrieved from

http://www.justiceinspectorates.gov.uk/hmicfrs/media/a-review-of-the-august-2011disorders20111220.pdf

Hoffman, P. (2018). Cadre deployment: *The* underlying cause of state capture. *Daily Maverick.* https://www.dailymaverick.co.za/opinionista/2018-05-14-cadre-deployment-the-underlyingcause-of-state-capture

Hoti, E. (2015). The technological, organizational and environmental framework of IS innovation adaption in small and medium enterprises: Evidence from research over the last 10 years. *International Journal of Business and Management*, *III*(4), 1–14. https://doi.org/10.20472/BM.2015.3.4.001

Huggler, J. (2016). Extremist violence increasing in Germany, warns report. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/2016/06/28/extremist-violenceincreasing-in-germany-warns-report

Hulnick, A. S. (2006). What's wrong with the Intelligence. Cycle. *Intelligence and National Security*, *21*(6), 959–979. https://doi.org/10.1080/02684520601046291

Human Rights Commission. (2024). *July's people the national investigative hearing report into the July 2021 unrest in Gauteng and KwaZulu Natal. South Africa,* p. 29. Human Rights Publication.

Intan Salwani, M., Marthandan, G., Daud Norzaidi, M., & Choy Chong, S. (2009). E-commerce usage and business performance in the Malaysian tourism sector: Empirical analysis. *Information Management and Computer Security*, *17*(2), 166–185. https://doi.org/10.1108/09685220910964027

Internet live stats. (2019). https:. Internet live stats – Internet usage & social media statistics. http://www.internetlivestats.com/

Internet live stats. (2021). https:. Internet live stats – Internet usage & social media statistics. Retired from http://www.internetlivestats.com/

Interpol. (2019). https:. http://www.interpol.int/Crimes/Terrorism/Analysing-social-media

Interpol. (2021). https:. http://www.interpol.int/Crimes/Terrorism/Analysing-social-media

Jain, P. N., & Vaidya, A. S. (2021). Analysis of social media based on terrorism: A review. *Vietnam Journal of Computer Science*, *8*(1), 1–21. https://doi.org/10.1142/S2196888821300015

Jakobsen, T. (2013). Theory of science – What is positivism? [Online]. *Popular Social Science*. http://www.popularsocialscience.com/2013/02/15/theory-of-science-what-ispositivism

Janssen, M., & Joha, A. (2011). Challenges for adopting cloud-based software as a service (SAAS) in the public sector. *19th European Conference on Information Systems*, ECIS 2011.

Jervis, R. (2006). Reports, politics, and intelligence failures: The case of Iraq. *Journal of Strategic Studies*, *29*(1), 3–52. https://doi.org/10.1080/01402390600566282

Johansen, P. A. (2011). Stadig mer Norsk spionasje. *Aftenposten*. https://www.aftenposten.no/norge/i/9O03r/Stadig-mer-norsk-spionasje

Johnson, D. E. (2006). *Learning large lessons: The evolving roles of ground power and air power in the post-cold war era. MG–405–AF*. RAND.

Johnston, B. (2021). Social media: The new intelligence collection platforms. *United Service*, *72*(4).

Kadushin, C. (2012). *Understanding social networks: Theories, concepts and findings*. Oxford Press.

Kamiński, M. A. (2019). Intelligence sources in the process of collection of information by the U.S. Intelligence Community. *Security Dimensions*, *32*(32), 82–105. https://doi.org/10.5604/01.3001.0014.0988 Sects. 82–105.

Kannabiran, G., & Dharmalingam, P. (2012). Enablers and inhibitors of advanced information technologies adoption by Smes: An empirical study of auto ancillaries in India. *Journal of Enterprise Information Management*, *25*(2), 186–209. https://doi.org/10.1108/17410391211204419

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, *53*(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Karahanna, E., Xin Xu, S. X., Xu, Y., & Zhang, N. (2018). The needs-affordances-features perspective for the use of social media. *MIS Quarterly*, *42*(3), 737–756. https://doi.org/10.25300/MISQ/2018/11492

Katz, B. (2020). The collection edge. *Harnessing Emerging Technologies for Intelligence Collection*. https://www.csis.org/analsis/collection-edge-harnessing-emerging-technologies-intelligence-collection

Kelion, L. (2014). Snowden leaks: GCHQ "spied on Facebook and YouTube". *BBC News*. https://www.bbc.com/news/technology-25927844

Kent, S. (1966). *Strategic intelligence for American world policy*. Princeton University Press. https://doi.org/10.1515/9781400879151

Khan, I. (2022). Zelenskyy humanizes Ukraine's plight in his social media messaging. *CNET*. https://www.cnet.com/news/politics/zelenskyy-humanizes-ukraines-plight-in-his-social-mediamessaging

Khayer, M. S. (2020). Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach. *Technology and Society*, *60*.

Koenig, M. & Murray. (2022). U.N. OFF. Of the high comm'r for Hum. *Berkeley protocol on digital open source investigations, U.N.* Doc. HR/PUB/20/2, U.N. Sales No. E.20.XIV.4. http://advocacyassembly.org/en/courses/58/#/chapter/1/lesson/1

Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). INTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics*, *10*(7), 818. https://doi.org/10.3390/electronics10070818

Koloveas, P., Chantzios, T., Tryfonopoulos, C., & Skiadopoulos, S. (2019). A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence. *In Proceedings of the 2019 IEEE World Congress on Services* (pp. 3–8). Milan, Italy, July 2023. https://doi.org/10.1109/SERVICES.2019.00016

Kubovich, Y. (2016). The Facebook squad: How Israel police tracks activists on social media. Retrieved from https://www.haaretz.com/israel-news/.premium-how-israel-police-tracks-activists-onsocial-media-1.5400741

Kuhns, W. J. (2004). Intelligence failures: Forecasting and the lessons of epistemology. *In Paradoxes of strategic intelligence* p. 3. Routledge.

Landsbergen, D., & Wolken, G. (2001). Realizing the promise: Government information systems and the fourth generation of information technology. *Public Administration Review, 61*(2), 206–220. https://doi.org/10.1111/0033-3352.00023

Lang, M. (2017). Social media monitoring continues to concern civil rights groups. Retrieved from http://www.govtech.com/public-safety/Social-Media-Monitoring-Continues-to-Concern-CivilRights-Groups.html

Le Sceller, Q., Karbab, E. B., Debbabi, M., & Iqbal, F. (2017). *Sonar: Automatic detection of cyber security events over the twitter stream*. Ares.

Lee, M. K. O., & Cheung, C. M. K. (2004). Internet retailing adoption by small-tomedium sized enterprises (SMEs): A multiple-case study. *Information Systems Frontiers*, *6*(4), 385–397. https://doi.org/10.1023/B:ISFI.0000046379.58029.54

Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th ed.). Pearson.

Lekhanya, L. M. (2013). Cultural influence on the diffusion and adoption of social media technologies by entrepreneurs in rural South Africa, Int. *Business and Economics Research Journal*, *12*(12), 1563.

Letsatsi-Duba, D. (2018). Budget vote speech of the Department of State Security by Hon. D. Letsatsi-Duba M.P., Minister of State Security. Retrieved from http://www.ssa.gov.za/Portals/0/SSA%20docs/Speeches/2022/MIN_Budget%20Vote%20Speech%2022%20May%2022.pdf

Liaropoulos, A. (2013). The challenges of social media intelligence for the intelligence community. *Journal of Mediterranean and Balkan Intelligence*, January, 5–14.

Liu, W., Sidhu, A., Beacom, A. M., & Valente, T. W. (2017). The international encyclopedia of media effects. *The International Encyclopedia of Media Effects* (pp. 1–12). John Wiley & Sons. https://doi.org/10.1002/9781118783764.wbieme0092

Lněnička, M., Nikiforova, A., Saxena, S., & Singh, P. (2022). Investigation into the adoption of open government data among students: The behavioural intention-based comparative analysis of three countries. *Aslib Journal of Information Management*, *74*(3), 549–567. https://doi.org/10.1108/AJIM-08-2021-0249

Locke, E., & Baum, J. (2004). The psychology of entrepreneurship. *Journal of Small Business Management*, *40*, 312–330.

Louw, M. (2014), Chapter 18: Ethics in Research. Juata & company Ltd. *In Research matters* (1st ed.) (pp. 262–273). Cape Town.

Lowenthal, M. M. (2006). *Intelligence: From secrets to policy*. CQ Press.

Lowenthal, M. M. (2019). *Lecture at the Norwegian Intelligence School*. Oslo.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy*. CQ Press.

Lowenthal, M. M., & Clark, R. M. (2015). *The five disciplines of intelligence collection*. CQ Press/Sage Publications.

Lumpp, T. G. (2014). *The effects of social media on national security within the United States*. Utica College.

Lundblad, J. P. (2003). A review and critique of Rogers' diffusion of innovation theory as it applies to organizations'. *Organization Development Journal*, *21*(4), 50.

Mahlase, M. (2018). Analysts divided as Ramaphosa brings back Mbeki securocrats to probe State Security Agency. Retrieved from https://www.news24.com/SouthAfrica/News/analysts-divided-asramaphosa-brings-back-mbeki-securocrats-to-probe-state-security-agency-20180615

Mahood, L.. M. (2015). SOCMINT: Following and liking social media. *Intelligence, 25*.

Maniscalco, M. L. (2012). Living in the cyber era: Reflections on security in a hybrid world. *The Mediterranean council for intelligence studies yearbook*. http://www.rieas.gr/images/mcis2012.pdf

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. http://www.rand.org/t/rr1742

Margolis, G. (2013). The lack of HUMINT: A recurring intelligence problem, global. *Security Studies*, *4*(2), 43–60. http://globalsecuritystudies.com/Margolis%20Intelligence%20(ag%20edits).pdf

Markham, N. (2015). ISIS supporters have more Twitter followers than you. *Vocativ*. http://www.vocativ.com/world/isis-2/isistwitter-census/

McLoughlin, L., Ward, S., & Lomas, D. W. B. (2020). Hello, world: GCHQ, Twitter and social media engagement. *Intelligence and National Security*, *35*(2), 233–251. https://doi.org/10.1080/02684527.2020.1713434

McQuail, D. (2010). *Mass communication theory*. Sage Publications.

Medina, R. M. (2014). Social network analysis: A case study of the Islamist terrorist network. *Security Journal*, *27*(1), 97–121. https://doi.org/10.1057/sj.2012.21

Moe, W. W., & Schweidel, D. A. (2014). *Social media intelligence*. Cambridge University Press. https://doi.org/10.1017/CBO9781139381338

Moffett, L., Oxburgh, G., Dresser, P., Watson, S., & Gabbert, F. (2021). Inside the Shadows: A survey of UK HUMINT practitioners examining their considerations when handling a Covert Human Intelligence Source (CHIS). *Psychiatry, Psychology and Law*, *29*, 1–19.

Mokoka, M. (2021). Meet the instigators: The Twitter accounts of the RET forces network that incited violence and demanded Zuma's release. *Daily maverick.* https://www.dailymaverick.co.za/article/2021-07-25-meet-the-instigators-the-twitter-accounts-of-the-ret-forces-network-that-incited-violence-and-demanded-zumas-release

Momani, A. M. (2020). The unified theory of acceptance and use of technology: A new approach in technology acceptance. *International Journal of Sociotechnology and Knowledge Development*, *12*(3), 79–98. https://doi.org/10.4018/IJSKD.2020070105

Momi, R. (2021). SOCMINT: Social media intelligence a new discipline? – *Grey dynamics*. https://www.greydynamics.com/socmint-social-media-intelligence-a-new-discipline

Montagnese, C. C. A. (2012). Impact of social media on national security. Retrieved from http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Documents/Ricerche/2012/Stepi/social_media_20120313_0856.pdf

Moore, M. (2014). RIP RIPA? Snowden, surveillance, and the inadequacies of our existing legal framework. *The Political Quarterly*, *85*(2), 125–132. https://www.academia.edu/7895161/RIP_RIPA_Snowden_Surveillance_and_the_Inadequacies_of_our_Existing_Legal_Framework. https://doi.org/10.1111/1467-923X.12085

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. Public Affairs.

Mostert, J. (2017). *The use of technology in NIS [personal interview]*, *17*(July). Pretoria.

Muthiah, M., Huang, B., Arredondo, J., Mares, D., Getoor, L., Katz, G., & Ramakrishnan, N. (2015). *Planned protest modelling in news and social media*. Association for the Advancement of Artificial Intelligence.

Myers, M. D. (2009). *Qualitative research in business & management*. Sage Publications. https://doi.org/10.4135/9781036208417

National security commission on artificial intelligence, interim report (national security commission on artificial intelligence. (2019). *Com*/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view. Retrieved from https://drive.google

Ngai, E. W. T., Tao, S. S. C., & Moon, K. K. L. (2015). Social media research: Theories, constructs, and conceptual frameworks. *International Journal of Information Management*, *35*(1), 33–44. https://doi.org/10.1016/j.ijinfomgt.2014.09.004

Norge, B. (2010). *Dagbladet*. Retrieved from https://www.dagbladet.no/nyheter/norge-bruker-mer-penger-pa-spionasje/64521683

Norton-Taylor, R. (2012). Former spy chief calls for laws on online snooping. *The Guardian*. http://www.theguardian.com/technology/2012/apr/24/former-spy-chieflaws-snooping

Nygaard, R. L. (2014). How can human intelligence enhance collection in an era of UnManned technology and reduced personnel?, army Command and General Staff College Fort Leavenworth KS. *Overview of State-Sponsored Terrorism.* United States Department of State. https://www.state.gov/j/ct/rls/crt/2001/html/10249.htm

Oates, B. J. (2006). *Researching information system and computing*. Sage Publications.

Oates, B. J. (2009). *Researching information system and computing*. Sage Publications.

O'Brien, K. (2011). The South African intelligence services: From apartheid to democracy. *Routledge. 1948–2005* p. 201.

O'Connell, K. M. (2005). The role of science and technology in transforming American intelligence. *In P. Berkowitz (Ed.), The future of American intelligence* (pp. 139–174). Hoover Institution Press.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research, Sprouts: Work. Papers. *Information Systems*, *10*(26), 1–46.

Oliveira, T., & Martins, M. R. O. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, *14*(1), 110–121.

Oliveira, T., Martins, R., Sarker, S., Thomas, M., & Popovič, A. (2019). Understanding SaaS adoption: The moderating impact of the environment context. *International Journal of Information Management*, *49*, 1–12. https://doi.org/10.1016/j.ijinfomgt.2019.02.009

Omand, D. (2017). Social media intelligence (SOCMINT). *The Palgrave handbook of security, risk and intelligence* (pp. 355–371).

Omand, D., Bartlett, D., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and national security journal*, *27*(6), 801–823.

Omede, A. J. (2015). Social media: A trend or threat to democracy. *Jorind*, *13*(1), 272–278. http://www.transcampus.org/jorindv13jun2015/jorind%20vol13%20no1%20jun%20chapter31.pdf

Pallaris, C. (2008). Open source intelligence: A strategic enabler of national security. *Center for Security Studies*, (32). http://www.isn.ethz.ch/isn/DigitalLibrary/Publications/Detail/?lng=en&id=50169

Patel, F., Rachel, L. W., Sophia, D., & Raya, K. (2019). Social media monitoring: How the department of homeland security uses digital data in the name of national security. *Brennan Center for justice*. https://www.brennancenter.org/publication/social-media-monitoring

Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide*. Blackwell Publishers. https://doi.org/10.1002/9780470754887

Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., & Britten, N. (2006). Guidance on the conduct of narrative synthesis in systematic reviews. *edu/viewdoc*/download?doi=10.1.1.178.3100&rep=rep1&type=pdf. http://citeseerx.ist.psu

Privacy International. (2017). *Social media intelligence*.

Putter, D., & Henrico, S. (2022). Social media intelligence: The national security–privacy nexus. *Scientia Militaria, 50*(1). Retrieved from https://doi.org/10.5787/50-1-1345

Ractham, V. V., & Srisamran, P. (2018). Effects of knowledge articulation and self-reflection on team performance. *Knowledge Management and E-Learning An International Journal*, *10*, 177–195.

Ramakrishnan, N., Butler, P., Muthiah, S., Self, N., Khandpur, R., Saraf, P., Wang, W., Cadena, J., Vullikanti, A., Korkmaz, G., Kuhlman, C., Marathe, A., Zhao, L., Hua, T., Chen, F., Lu, C. T., Huang, B., Srinivasan, A., Trinh, K., . . . Mares, D. (2014). Beating the news with embers: Forecasting civil unrest using open source indicators. *In Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. KDD'14 (pp. 1799–1808). http://doi.acm.org/10.1145/2623330.2623373. https://doi.org/10.1145/2623330.2623373

Ray, D. (2016). Cloud adoption decisions: Benefitting from an integrated perspective. *Electronic Journal of Information Systems Evaluation*, *19*(1), 3–21.

Resnik, R. (2011). What is ethics in research & why is it important? [Online] National Institute of Environmental Health Services. Retrieved from https://www.niehs.nih.gov/research/resources/bioethics/whatis/

Ressler, S. (2006). Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs*, *2*(2).

Rezk, D. (2017). The Arab world and western intelligence: Analysing the Middle East, 1956–*1981*. *Edinburgh University Press.* https://doi.org/10.3366/edinburgh/9780748698912.001.0001

Richelson, J. T. (2018). *US Intelligence Community*. 7th ed.

Rogers, E. M. (1962). *Diffusion of innovations*. The Free Press of Glencoe.

Ronn, K. V., & Soe, S. O. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, *34/3*, 363.

Rovner, J. (2013). Intelligence in the Twitter age. *International Journal of Intelligence and CounterIntelligence*, *26*(2), 260–271. https://doi.org/10.1080/08850607.2013.757996

Ruggiero, T. E. (2000). Uses and gratification theory in the 21st century. *Mass Communication and Society*, *3*(1), 3–37. https://doi.org/10.1207/S15327825MCS0301_02

Safari, F., Safari, N., & Hasanzadeh, A. (2015). The adoption of software-as-a-service (SaaS): Ranking the determinants. *Journal of Enterprise Information Management*, *28*(3), 400–422. https://doi.org/10.1108/JEIM-02-2014-0017

Safranek, R. (2012). The emerging role of social media in political and regime change. http://www.csa.com/discoveryguides/discoveryguides-main.php

SAS. (2012). *Using intelligence from social media to combat security threats*. SAS Institute.

Sauerwein, C., Fischer, D., Rubsamen, M., Rosenberger, G., Stelzer, D., & Breu, R. (2021). From threat data to actionable intelligence: An exploratory analysis of the intelligence cycle implementation in cyber threat intelligence sharing platforms. *The 16th International Conference on Availability, Reliability and Security*, 1–9. https://doi.org/10.1145/3465481.3470048

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.).

Schaurer, S., & Jorger, J. (2010). The evolution of Open Source Intelligence. *OSINT research reports*, 3/2010 ISN. Zurich, Switzerland.

Schwab, K. (2016). *The fourth Industrial Revolution*. World Economic Forum.

Scott, J. (2000). *Social network analysis: An introduction*. Sage Publications.

Scott, J. (2004). *Social network analysis: A handbook*. Sage Publications.

Sech, J., DeLucia, A., Buczak, A. L., & Dredze, M. (2020). Civil unrest on Twitter (CUT): A dataset of tweets to support research on civil unrest. *In Proceedings of the Sixth Workshop on Noisy User-Generated Text (W-NUT 2020)* (pp. 215–221), Online. Association for Computational Linguistics. https://doi.org/10.18653/v1/2020.wnut-1.28

Senekal, B., & A. (2018). SOCMINT: The monitoring of social media for community safety purposes within a big data framework in South Africa with specific reference to Orania. *Litnet*. https://www.litnet.co.za/socmint-the-monitoring-of-socialmedia-for-community-safety-purposes-within-a-big-data-framework-in-south-africawith-specific-reference-to-orania/

Sherry, J. L., & Boyan, A. (2008). Uses and gratifications. *In W. Donsbach (Ed.), The international encyclopedia of communication* (pp. 5239–5244). Blackwell Publishing. https://doi.org/10.1002/9781405186407.wbiecu011

Shiau, W.-L., Hsu, P.-Y., & Wang, J.-Z. (2009). Development of measures to assess the ERP adoption of small and medium enterprises. *Journal of Enterprise Information Management*, *22*(1/2), 99–118. https://doi.org/10.1108/17410390910922859

Shulsky, A. N. (1995). What is intelligence? Secret and competition among states. In R. Godson, E. May, & G. Schmitt (Eds.), *US intelligence at the crossroads. Washington: Brassey*‟s. p. (pp. 17–27).

Shulsky, A. N., & Schmitt, G. T. (2002). *Silent warfare: Understanding the world of intelligence. Dulles*. Potomac Books.

Simferopolnovosti. (2021). Russian reply. Retrieved from https://www.instagram.com/p/CNE5MLypCb6/

Singh, H. S., & Laura, S. S. (2014). Indian police arrest man suspected of running pro-ISIS Twitter account. *CNN*. http://edition.cnn.com/2014/12/13/world/asia/india-isis-twitter-arrest/

Singh, J. (2012). *Media and national security*. Knowledge World Publishers.

Sivathanu, B., & Pillai, R. (2019). Leveraging technology for talent management: Foresight for organizational performance. *International Journal of Sociotechnology and Knowledge Development, 11*(2), 16–30. https://doi.org/10.4018/IJSKD.2019040102

Smyth, S., Houghton, C., Cooney, A., & Casey, D. (2012). Students' experiences of blended learning across a range of postgraduate programmes. *Nurse Education Today, 32*(4), 464–468. https://doi.org/10.1016/j.nedt.2011.05.014

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

South Africa. (1983). Republic of South Africa constitution act 110 of 1983. https://law.wisc.edu/gls/cbsa2.pdf

South Africa. (1994). *National strategic intelligence act 39 of 1994*.

South Africa. (1995). *White paper on intelligence.*

South Africa. (2002). Regulation of Interceptions of Communications and Provision of Communication – Related information (RICA) Act 70 of 2002.

South Africa. (2018*). President Ramaphosa appoints high-level review panel on State Security Agency. State Security Agency.*

http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2018/President%20appoints%20review%20panel_15June2018.pdf

South Africa. (2021). *South African Human Rights Commission*. GILAB Act.
South Africa. (2021). Report of the expert panel into the July 2021 civil unrest. https://www.thepresidency.gov.za/content/report-expert-panel-july-2021-civil-unrest. Date of access: 25 July 2022

Sparrow, M. K. (1991). Network vulnerabilities and strategic intelligence in law enforcement. *International Journal of Intelligence and CounterIntelligence*, *5*(3), 255–274. https://doi.org/10.1080/08850609108435181

Statista. (2024). The statistics portal for market data. *Statista – The statistics portal for market data, market research and market studies*. https://www.statista.com/

Stefanidis, A., Crooks, A., Radzikowski, A., Croitoru, A., & Rice, M. (2014). Social media and the emergence of open-source geospatial intelligence. *In Human Geography: Socio-Cultural Dynamics and Global Security: Socio-Cultural Dynamics and Challenges to Global Security*. (USGIF), 109–123.

Stegen, J. I. (2019). Social Media Intelligence (SOCMINT) within the South African context: *A theoretical and strategic framework for the national security environment*. Reposity. nwu.ac.za

Stensile, S. (2023). Intelligence warning and revolution: Lessons from the Arab Spring. *Journal of Security, Intelligence, and Resilience Education*.

Swart, H. (2011). Secret state: How the government spies on you. Retrieved from http://amabhungane.co.za/article/2011-10-14-secret-state

Swart, H. (2016). Communications surveillance by the South African Intelligence Services. Retrieved from https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-niaswart_feb2016.pdf

Swart, H. (2018). Government surveillance of social media is rife. Guess who‟s selling your data? *Daily Maverick.* https://www.dailymaverick.co.za/article/2018-04-25-government-surveillance-ofsocial-media-is-rife-guess-whos-selling-your-data/#.WvmUl6SFOM8

Tannam, E. (2017). British intelligence allegedly using social media for mass surveillance. Retrieved from https://www.siliconrepublic.com/enterprise/uk-social-media-surveillance

Tarafdar, M., & Vaidya, S. D. (2006). Challenges in the adoption of e-commerce technologies in India: The role of organizational factors. *International Journal of Information Management*, *26*(6), 428–441. https://doi.org/10.1016/j.ijinfomgt.2006.08.001

Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In K. E. Himma & H. T. Tavani (Eds.), *The handbook of information and computer ethics* (pp. 131–164). John Wiley & Sons. https://doi.org/10.1002/9780470281819.ch6.

Tetlock, P. E., & Gardner, D. (2005). *Superforecasting: The art and science of prediction*. Crown Publishing Group.

Theohary, C., & Rollins, J. (2011). Terrorist use of the internet: Information operations in cyberspace. Retrieved from http://www.fas.org/sgp/crs/terror/R41674.pdf

Thompson, R. (2011). Radicalization and the use of social media. *Journal of Strategic Security*, *4*(4), 167–190. https://doi.org/10.5038/1944-0472.4.4.8

Toews, R. (2022). Synthetic data is about to transform artificial intelligence. *Forb.* https://www.forbes.com/sites/robtoews/2022/06/12/synthetic-data-is-about-to-transform-artificialintelligence/

Toffler, A. (2022). *Powershift: Knowledge, wealth, and power at the edge of the 21st century*. Random House Publishing Group: Bantam Books.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Treverton, G. (2018). Reshaping intelligence for an age of terror: Where do we stand? [Web]. *Spring*. http://mit.edu/ssp/seminars/wed_archives

Tripathy, J. P. (2013). Secondary data analysis: Ethical issues and challenges [Online]. *Iranian Journal of Public Health*, *42*(12), 1478–1479. (PubMed Central). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4441947/

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 Hulst, R. C. (2009). Introduction to social network analysis (SNA) as an investigative tool. *Trends in Organized Crime*, *12*(2), 101–121. https://doi.org/10.1007/s12117-008-9057-6

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-andsocial-media-is-big-brother-following-you/

Van Dyk, R., & Van Belle, J. P. (2019). Factors influencing the intended adoption of digital transformation*: A South African case study. S.l.* (pp. 519–528). IEEE.

Vandiver, J. (2021). EUCOM raises threat level for Ukraine as Russia builds up forces. *Stars and Stripes*. https://www.stripes.com/theaters/europe/eucom-raises-threatlevel-for-ukraine-as-russia-builds-up-forces-1.667998

Ven, K., & Verelst, J. (2011). An empirical investigation into the assimilation of open source server software. *Communications of the Association for Information Systems*, *28*(9), 117–140. https://doi.org/10.17705/1CAIS.02809

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). *User acceptance of information technology: Toward a unified view, MIS quarterly, 27*(3), pp. 425-4.

Vhumbunu, C. H., Rudigi, J. R., & Mawire, C. (2022). Addressing xenophobia through Peacebuilding processes in South Africa: Successes, challenges and prospects. *African Journal of Peace and Conflict Studies* (formerly Ubuntu: Journal of Conflict and Social Transformation), *11*(2).

Wamba, S. F., & Carter, L. (2014). Social media tools adoption and use by SMEs: An empirical study. *Journal of Organizational and End User Computing*, *26*(2), 1–17. https://doi.org/10.4018/joeuc.2014040101

Wankhade, M., Rao, A. C. S., & Kulkarni, C. (2022). A survey on sentiment analysis methods, applications, and challenges. *Artificial Intelligence Review*. https://link.springer.com/article/10.1007/s10462-022-10144-1

Wasserman, S., & Faust, K. (1994). Social network analysis: Methods and applications. *Cambridge University Press*. https://doi.org/10.1017/CBO9780511815478

We are social & Hootsuite. (2018). Digital in 2018. Retrieved from https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018 Date of access: August 3, *13*, 2022

Weinbaum, C., Berner, S., & McClintock, B. (2017). SIGINT for anyone: The growing availability of signals intelligence in the public domain. Retrieved from https://www. http://rand.org/pubs/perspectives/PE273.html

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into business transformation*. Harvard Business Review Press.

White, H. C., Scott, A., Boorman, R., & Breiger, L. (1976). Social structure from multiple networks: Blockmodels of roles and positions. *American Journal of Sociology*, 81730–81779.

Whiting, A., & Williams, D. (2013). Why people use social media: *A uses and gratification approach*, 6776.*16*(4), 362–369. https://doi.org/10.1108/QMR-06-2013-0041

Williams, H., & Blum, I. (2018). *Defining second generation Open Source Intelligence (OSINT) for the defense enterprise*. Rand Corporation.

Wintour, C. (2000). Islamic State propaganda, terrorism Monitor. *Volume*, *13*(12).

Wisdom, J. P., Chor, K. H. B., & Hoagwood, K. E. (2014). Innovation adoption: a review of theories and constructs, Adm. *Policy Ment. Heal. Ment. Heal. Serv*. 41, (4), pp. 480–502.

World Economic Forum. (2020). Chapter 1. The future of jobs and skills. In *org/future-of-jobs-2022/chapter-1-the-future-of-jobs- and-skills*. http://reports.weforum

Wu, J., Yuen, C., Cheung, N. M., Chen, J., & Chen, C. W. (2015). Enabling adaptive high-frame rate video streaming in mobile cloud gaming applications. *IEEE Transactions on Circuits and Systems for Video Technology*, *25*(12), 1988–2001.

Yin, R. K. (2009). *Case Study Research: Design and Methods* (4th ed.). Sage Publications.

Yoon, T., & George, J. (2013). Why aren't organizations adopting virtual worlds? *Computers in Human Behavior*, *29*, 772–790.

Yu, S. (2023). Social media intelligence: AI applications for criminal investigation and national security. In *Handbook of research on artificial intelligence applications in literary works and social* (pp. 152–170). IGI Global, 2023.

Yucel, S. (2018). Modeling digital business strategy. *International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 209–214). Las Vegas.

Zheng, S., Yen, D. C., & Tarn, J. M. (2000). The new spectrum of the cross-enterprise solution: The integration of supply chain management and enterprise resource planning systems. *Journal of Computer Information Systems*, *41*(1), 84–93. https://doi.org/10.1080/08874417.2000.11646980

APPENDIX A: ETHICAL CLEARANCE CERTIFICATE

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

SCHOOL OF BUSINESS SCIENCES ETHICS COMMITTEE
CONSTITUTED UNDER THE UNIVERSITY HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)

CLEARANCE CERTIFICATE	**PROTOCOL NUMBER: CBUSE2177**
PROJECT TITLE	The role of trust and risk in the adoption of super apps in Challenges of adopting Social Media Intelligence (SOCMINT) as a tool for mitigating national security threats in South Africa - The July 2021 unrest case study.
INVESTIGATOR	Bridget Vulani Rikhotso
SCHOOL/DEPARTMENT OF INVESTIGATOR	School of Business Sciences
DATE CONSIDERED	02 February 2024
DECISION OF THE COMMITTEE	Approved Unconditionally
RISK LEVEL	Low Risk
EXPIRY DATE	31 December 2027

ISSUE DATE OF CERTIFICATE 07 February 2024 **CHAIRPERSON** _____
(Neetu Ramsaroop)

cc: Supervisor: Kebashnee Moodley

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

_____ 07/01/2024
Signature **Date**

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

APPENDIX B: PARTICIPATION INFORMATION



University of the Witwatersrand,
School of Business Sciences

<Participant Name>
<Participant Position>
<Participant Address>

<Date>

Dear Sir/Madam,

RE: Research Cover letter for Interview

My name is Bridget RIKHOTSO, I am pursuing a Master's Degree in Information Systems in the School of Business Sciences at the University of the Witwatersrand. To fulfil a crucial requirement of the Master's programme, I have to undertake an academic research project under the supervision of Dr. Kebashnee Moodley.

The purpose of this interpretive study is to explore the challenges of adopting Social Media Intelligence (SOCMINT) as a tool for mitigating national security threats because of the failure to predict or prevent the July 2021. I am researching "Challenges of Adopting Social Media Intelligence (SOCMINT) as a tool for Mitigating National Security Threats in South Africa - The July 2021 Unrest Case Study".

Social media technologies and capabilities are transforming intelligence collection methods as they bring with them new ways of mitigating national security threats. However, the South African intelligence community is not fully utilising SOCMINT for intelligence gathering.

Their failure in recognising SOCMINT as an intelligence collection discipline resulted in one of the country's intelligence failures in history, the July 2021 civil unrest. Intelligence services have a notoriously poor track record in anticipating unrests and revolutions. South Africa's July 2021 civil unrest is no exception.

The purpose of this interpretive study is to explore the challenges of adopting Social Media Intelligence (SOCMINT) as a tool for mitigating national security threats as a result failing to predict or prevent the July 2021 unrest. The TOE theory integrated with the UTAUT theory was used to guide the study.

The researcher believes in multiple realities to understand all perspectives of the realities; hence the qualitative methodology was the chosen approach for this study. Qualitative methods, such as interviews will enable the researcher to explore the intelligence community's perspective and views of their experience and use of SOCMINT as an intelligence collection discipline. Given the problems and the cleavages in South Africa's society, it is unlikely that the country will not experience outbursts of riots and looting. Since South Africa has experienced economic and social unrest ever since the country transitioned to democracy in 1994, this study will provide recommendations on systems that need to be put in place to forewarn and eventually respond to unrest or similar occurrences that may pose a threat to national security.

A sampling strategy will be based on the non-random selection of Intelligence Community (IC) and retired officials who have SOCMINT expertise and knowledge. The interviews will be semi-structured in nature because they combine the components of both structured and unstructured interviews. The interview will take place in less than 1 hour outside working hours; thus, it will not disturb their official duties. All participants will not be expected to disclose classified information because of the sensitive nature of the environment. The "need-to-know" principle will be applied throughout the process.

Participants will be asked to give their written or verbal consent before the research begins. Their responses will be treated confidentially, and identities (their names and the name of the organisation) will be anonymous. Individual privacy will be maintained in all published and written data resulting from the study.

The results will be communicated in a dissertation to the University of the Witwatersrand and may be provided to the intelligence community if requested.

The research participants will not be advantaged or disadvantaged in any way. They will be reassured that they can withdraw their permission at any time during this project without any penalty. There are no foreseeable risks in participating in this study. The participants will not be paid for this study.

Thank you in advance for your participation, should you have any queries or concerns, please do not hesitate contact either myself at 2514770@students.wits.ac.za alternatively send an email to my supervisor: email kebashnee.moodley@wits.ac.za.

Yours sincerely,

Bridget Vulani RIKHOTSO
0737276309
2514770@students.wits.ac.za

APPENDIX C: INTERVIEW SCHEDULE

The questions included in this interview mostly address elements relevant to the use of SOCMINT in the South African Intelligence Community. Written consent must be obtained by you (participant) stating that you voluntarily took part in the interviews. The interview with you will involve the following questions. All questions will be asked during the three sections of the interview, which should take about an hour.

SECTION 1: PARTICIPANT'S BACKGROUND

1.1 What is your understanding of Social Media Intelligence (SOCMINT) and its use to mitigate national security threats?

1.2 What experience do you have in terms of SOCMINT as a decision maker, implementer or user?

1.3 How long have you been involved in any SOCMINT related activity within the organisation?

SECTION 2: UNDERSTANDING OF SOCMINT

2.1 What is the organisation's view, when it comes to utilising SOCMINT as an intelligence discipline?

2.2 Is SOCMINT recognised as a legitimate intelligence discipline within the Intelligence Analysis Community, and if not—why?

2.3 Do you believe SOCMINT can be used to effectively detect an emerging threat, please elaborate on your answer? Do you believe information of national interest can be derived from the use of SOCMINT?

2.4 If SOCMINT was to be adopted as an intelligence discipline, do you believe this technology would improve the intelligence product? Explain.

2.5 What benefits do you think SOCMINT will bring to the organisation?

2.6 What impact does SOCMINT have on national security?

2.7 How important is it for an organisation to adopt SOCMINT?

2.8 Which South African legislation has an impact on how SOCMINT is used by the country's intelligence services and organisations?

2.9 Are there clear guidelines in SA legislation regarding the application of SOCMINT for domestic national security?

SECTION 3: MAIN RESEARCH QUESTIONS

3.1 TECHNOLOGY

3.1.1 In your opinion, what are the factors that the organisation needs to investigate or consider or put in place in the development, implementation and eventual adopting SOCMINT?

3.1.2 Are there risks in the deployment of SOCMINT as an intelligence collection discipline? If there are risks, what are risks and how can the risks be mitigated?

3.1.3 What are some of the key challenges that you foresee in SOCMINT adoption in the intelligence community"?

3.1.4 What are the causes/reasons for the possible existing challenges?

3.2 ORGANISATION

3.2.1 What do you believe is top management's role of SOCMINT adoption in the organisation? What have you observed in this regard?

3.2.2 What interventions are utilised to train and upskill employees for SOCMINT adoption and implementation?

3.3 EVIRONMENT

3.3.1 What is different about your organisation's approach to SOCMINT adoption when compared with other intelligence organisations?

3.3.2 What lessons can be drawn that can help the intelligence community to be in a better position to warn of future unrest?

3.3.3 Do you think it was possible for the intelligence community to anticipate the violence during the July unrest with social media?

3.3.4 In your own opinion, why do you think the intelligence community was unable to anticipate the unrest?

3.3.5 What can be done to avoid the possibility of such events happening again?

APPENDIX D: ILLUSTRATION OF TRANSCRIBED INTERVIEW AND CODING

Question	**1. MAIN RESEARCH QUESTIONS** Why is the adoption of SOCMINT in the South African intelligence community relatively low, and what challenges are presented by SOCMINT? (Specific focus on the July 2021 unrest). 1.1 What are the primary obstacles to recognising SOCMINT as an official intelligence collection discipline within the intelligence community? 1.2 What factors impede the effective adoption of SOCMINT, and what challenges are encountered during its execution? 1.3 What extent of information was accessible to the intelligence services to adequately detect, comprehend, and respond to both the threat and the actual outbreak of the July 2021 unrest violence?						
High-Level THEME	TECH-SECURITY	ADOPTION	ORG-MANAGEMENT SUPPORT	ORG-TECH INCLINATION	ENV-SILOS/ Coordination	ENV-GOVERNMENT REGULATION	IND-SKILL/ TRAINING
Themes	TechSec	Ado	OrgMs	OrgTI	EnvSil	EnvGr	IndST
Codes	- P#4, P#5, P#6, P#7, P#8: Information Security - data privacy and protection as factors of concern. The GILAB Act seeks to counter the challenges of abusing power, privacy, and data security >**TechSeDP** -P#6, P#7, P#8, P#9, P#10: Involvement of third-party entities leading to loss of control > **TechSecSC**	-P#3: Technology alignment with the organisation' s mandate >**AdoDecStr** -P#1: Information Security > **AdoDecSec** **-P#1:** SOCMINT is being urged by the fourth industrial revolution **>AdoDecAI** -P#7: Social media weapomisation >AdoDecL	-P#1, P#2, -P#3, -#P10-P#12: Politicisation of the intelligence > **OrgMsPoli** -P#1, P#11, P#12, Unstable leadership, Ministers and management interfering in operational issues >**OrgMsUl**	-P#2, P#4, P#10: Technological know-how, training and processes > **OrgTITkw** -P#5, P#8, P#10, Cost Management **>OrgTICm**	-P#3, P#9, P#10, P#11, P#12: Inconsistent information and interpretation of information and threat >**EnvSilNalStr** #P4, #P8, P#9: lack of coordination and approach to the July unrest > **EnvSilNalCor**	-P#4, P#5, P#9, P#12: probing into Social media regulation >**EnvGrAp** -P#4, P#8, P#9: No regulation governs the use of SOCMINT in South Africa >**EvnGrIn**	-P#2, P#4: analytics resource skill would be able to execute SOCMINT solutions >**IndSTR** -P#2, P#3, P#10, P#11: Inadequate training in law enforcement and intelligence agencies impedes prompt action and efficient crisis management >**IndSTRT**
REFERRED DOCUMENTS	GILAB Act, 2024		High Review Panel Report		Military National Security Strategic Act	Rica Act	High Review Panel report
Participant #4	*The criticisers of SOCMINT may argue that retaining social media data for long periods of time increases the risk of misinterpretation and reputational damage. There is a belief that bulk surveillance and data collection through social media platforms create*	*SOOMINT can be useful in giving situational awareness in the aftermath of an incident, but the risks posed by false information and misinformation contradict most of its conceptual usefulness, and most of the intelligence*	*One of the reasons why SOCMINT was not recognised as an intelligence collection discipline is because the politicisation of the environment resulted in a prolonged regulating of the social of media.*	*In order for the organisation's personnel as a whole to be able to utilise SOCMINT efficiently or support it effectively as well, they must undergo thorough training as part of our digital transformation.* A *detailed customised*	*Silos approach is caused by competitiveness within the community and leaders wanting individual glory*	*The regulation initiatives were also met with reactions from the social media community.* *Since we do not have a legislation that governs the use of SOCMINT, the RICA Act was passed to prevent mischief involving the interception of communication. Under*	*Social media intelligence requires Data Science and predictive analytics knowledge which is rare skill.* *It is important to partner with other training institutes within government, such as the training*

	additional threats to managing and keeping the data secure.	*communities might lack some of the necessary resources or requirements to operate a situational awareness capability effectively*.		*training, ongoing upskilling, knowledge transfer by service providers, and learning from the private sector are few of the human resource interventions which can be used by the intelligence community for SOCMINT adoption inclination*".		*RICA, the state would have had a general legal protection to carry out SIGINT and SOCMINT intelligence activities. This is because RICA was aimed to control the manner in which intelligence services conduct their operations. But because of the Constitution Court ruling, the communicatio n centres like National Communicatio n Centre were found wanting.*	*entities in Crime Intelligence, Department of Defence, Department of Internationa l Relations and Corporation (DIRCO) Academy, the National School of Government and others. This will ensure correct career pathing, extensive knowledge and understandi ng of any new technology that will advance intelligence capabilities.*

THEME	**SUB THEME**	**HIGH LEVEL CODE**	**CODE NAME**	**INTERVIEW QUESTION**	**RELEVANT DOC**	**COUNT**	**MENTIONED BY:**
ADOPTION	Adoption Decision	AdoDec	AdoDecStr	1.2, 1.2, 1.3, 2.2, 2.6		2	P#2, P#3
TECHNOLOGY	Compatibility	TechC	TechCC	2.3, 2.4		5	P#2, P#3, P#4, P#10, P#11
TECHNOLOGY	Simplicity	TechSi	TechSiS	2.5		2	P#2, P#4
TECHNOLOGY	Expectancy	TechE	TechEPo	3.1.1, 3.1.2, 3.1.4		4	P#4, P#6, P#7, P#9
TECHNOLOGY	Security	TechS	TechSecSc	3.1.2		8	P#3, P#4, P#5, P#6, P#7 P#8, P#9, P#10
ORGANISATION	Management Support	OrgMs	OrgMsPoli	2.1, 2.7, 3.2.1	High Review Panel Report	5	P#1, P#2, P#3, P#11, P#12
ORGANISATION	Technology Inclination	OrgTI	OrgTITkw	3.1.3		4	P#2, P#4, P#10, P#12
ORGANISATION	Cost	OrgC	OrgMsC	3.1.4		5	P#1, P#5, P#8, P#10, P#11
ENVIRONMENT	Silos	EnvSil	EnvSilNalStr	3.3.1	High Review Panel Report	6	P#1, P#3, P#9, P#10, P#11, P#12
ENVIRONMENT	Government Regulations	EnvGr	EnvGrAp	2.8, 2.9	GILAB Act, Rica Act	6	P#3, P#4, P#5, P#8, P#9, P#12
ENVIRONMENT	Coordination	EnvC	EnvSilNalCo	3.3.3		5	P#1,P#3, P#9, P#10, P#12
INDIVIDUAL	Skills Shortage	IndSS	IndSTR	3.2.2		5	P#2, P#4, P#9, P#10, P#11
INDIVIDUAL	Training and Exposure	IndTE	IndSTRT	3.2.2		3	P#3, P#4, P#12

APPENDIX E: LETTER OF PERMISSION FROM INTELLIGENCE COMMUNITY

[redacted]
REPUBLIC OF SOUTH AFRICA

12 February 2024

[redacted]

Submission: Request to conduct research interviews with [redacted] officials for study purposes

1. ***Purpose***

The purpose of this submission is for the member to obtain approval to conduct interviews with members who are specialising in the Social Media Intelligence (SOCMINT) within the organisation for study purposes.

2. ***Executive Summary***

The member is currently enrolled for a Masters in Information system Degree, which is due to be completed soon at Wits University. The topic of the study is "Challenges of adopting Social Media Intelligence (SOCMINT) as a tool for mitigating national security threats in South Africa - The July 2021 unrest case study".

3.1 Background and Motivation

3.1.1 Challenges of adopting Social Media Intelligence (SOCMINT) as a tool for mitigating national security threats in South Africa - The July 2021 unrest case study. Popular social media sites like Facebook and Twitter began to emerge as significant routes for information exchange within the various extremis t communities. However, in South Africa, social media is a new discipline for intelligence gathering and the country

has been slow in recognising the value of SOCMINT as an intelligence collection discipline.

3.1.2 The researcher will not request the members to divulge classified or sensitive information that has to do with agency, individuals or operations, she will simply solicit the perspective of the members that have knowledge of SOCMINT.

3.1.3 As part of observing the University's ethical code of conduct and for the safety of the respondents; their names, ranks and structures within the organisation will not be divulged. In the study they will be presented on the basis of anonymity.

4. Formulation of the Problem

The member requests that the [redacted] should approve this submission in order to allow the member to proceed with oral interviews with targeted members. The identified members consist of the Divisional Heads and ordinary members who have knowledge in SOCMINT within the organisation. It is believed that this will assist the study to arrive at objective and balanced findings which will be able to provide workable recommendations to all interested parties.

5. ***Recommendations***

It is recommended that the [redacted] approves this submission to enable the member to conduct the requested interviews.

8. ***Compiler***

BV. RIKHOTSO

[redacted]

APPENDIX F: ILLUSTRATION OF CONSENT FORM

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Dear Respondent

Researcher: Bridget Vulani Rikhotso (0737276309) Email Address: 2451770@students.wits.ac.za
Supervisor: Dr. Kebashnee Moodley (011 717 8256) Email Address:kebashnee.moodley@wits.ac.za

"Challenges of adopting Social Media Intelligence (SOCMINT) as a tool for mitigating national security threats in South Africa - The July 2021 unrest case study".

Consent

I, …….., agree to participate in this research project.

I agree to the following:

(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES	NO
I understand that I can volunteer to take part in the study	YES	NO
I agree that direct quotations from my interview/focus group/other activity may be used by the researcher in their research report/ manuscript/book chapter	YES	NO
I agree that my participation will remain anonymous (my name or other identifying data will not be used by the researcher in their research report/manuscript/book chapter)	YES	NO

Hereby confirm that I fully understand the contents of this document and the nature of the research project and I consent fully to participating in the research project.

I understand that I am at liberty to withdraw from the project at any time, should I so desire.

…… (signature)
…… (name of participant)
…… (date)

APPENDIX G: TURNITIN

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Bridget Rikhotso
Assignment title:	Research Report
Submission title:	Final Dissertation 2514770.docx
File name:	Final_Dissertation_2514770.docx
File size:	1.6M
Page count:	154
Word count:	44,704
Character count:	267,072
Submission date:	12-Nov-2024 09:37PM (UTC+0200)
Submission ID:	2517398272

