AN EXPLORATION OF THE VARIABLES THAT ACT AS PREDICTORS OF INSIDER ESPIONAGE: A FIVE-FACTOR APPROACH

by

FRANK CHRISTIAN DANESY

Student Number: 64011348

submitted in fulfilment of the requirements for the degree

of

DOCTOR OF PHILOSOPHY

in the subject of

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISORS

Prof A. Velthuizen
Prof J.S. Horne

October 2022

DECLARATION OF AUTHENTICITY

Student Number: 64011348

Degree: Doctor of Philosophy in Criminal Justice

I, Frank Christian Danesy declare that “An exploration of the variables that act as predictors of insider espionage: A multisectoral perspective” is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

F.C. Danesy 19 September 2022

Signature Date

ACKNOWLEDGEMENTS

A research project of this magnitude and scope could not be completed without the direct and indirect support of many others who, through their interest, encouragement, and guidance, help the researcher to hold course. I express my sincere gratitude to:

- My academic supervisor, Prof A. Velthuizen, former Head of the Institute for African Renaissance Studies at the University of South Africa. Through his knowledge, experience, and wisdom and with his unwavering care, concern, and patience for my research, he provided me with invaluable support and guidance in all aspects and during all phases of this project. I am deeply grateful for all I have learned from him, not only with respect to conducting the research, and with respect to mentoring a research project. This will undoubtedly influence my work in the future.
- My academic co-supervisor, Prof J.S. Horne of the Department of Police Practice at the University of South Africa. She kindly accepted the co-mentorship of my research project, consistently offered unwavering care and concern, and patiently offered me invaluable advice which always pointed me in the right direction. I have learned much from her which I will carry forward into my future academic undertakings and I will always remain deeply indebted.
- To the University of South Africa, I gratefully acknowledge the opportunity to develop and enhance my knowledge and experience as a researcher and also for providing me with the unique opportunity to do so in a rich cultural setting. The experience of studying at this university has been invaluable.
- My family for their support and encouragement to work on this project and for taking my absences from family activities in strides. This project would simply not have been possible without their understanding and care.
- My wife, Dorothea, for her unwavering understanding for my desire to explore the unknown and to contribute to knowledge – an undertaking which meant further increasing the size of our already sizable private library.
- My oldest grandson, Tristan, who enjoyed discussing the subject of my research with me and who often amazed me with his insights despite his young years. I am so curious to see where his future will take him.

- My late mother, Marga Danesy, who was a librarian from whom I inherited my love for books. Both, she and my late grandmother, Alice Schröder, always believed in me and unconditionally supported and encouraged me in my quest to gain knowledge. They will always have a special place in my heart and mind.
- My friend and former colleague, Brigadier General Dr Thomas Reiter, former European astronaut and Director of Human Spaceflight and Operations at the European Space Agency, for our many inspiring discussions about space, aviation, and music; for also offering living proof that the sky is not the limit, and for rekindling my interest in matters related to security, which eventually led me to undertake this project.
- My friend and former colleague, Dr. Rolf Densing, Director of Operations at the European Space Agency, for our many inspiring discussions on strategy and thinking "outside the box". I know few others who are so capable of recognising and assessing the "big picture".
- My friend and former colleague, Stefano Zatti, former Head of Security at the European Space Agency, for our numerous inspiring discussions on matters related to organisational security and the protection of privileged information.
- Dr Paul Medhurst for his guidance during my master's studies in intelligence and counterintelligence at AMU. His substantial experience and profound knowledge of literature in these fields were instrumental in helping me become deeply familiar with the subject. It was through his exegetic insights that I had the foundation necessary to embark on this project.
- My colleague, Prof Torsten Biemann, Chair of Business Administration, Human Resource Management and Leadership at the University of Mannheim for being a sounding board in matters related to organisational psychology, particularly in the fields of motivation, counterproductive work behaviour, and testing. Our discussions have been invaluable in providing important impulses.
- Last, but certainly not least, my friends who frequently asked about the progress of my research and who look forward to hearing about the results. Often unaware that they were implicitly encouraging me to carry on in my academic endeavour, they also played an important role in the completion of this project.

ABSTRACT

Espionage has destabilised governments, jeopardised national security, imperilled key infrastructures, diminished the economic strength of nations, and cost lives. The problem addressed through this research premises on the often ineffective processes and underlying conceptual frameworks currently used to ferret out the afore-cited insider threats that are immanent in espionage. The present research, therefore, sets out to explore the crucial variables that act as predictors of insider espionage in governmental, intergovernmental, and industrial organisations; the inter-relatedness of these variables; as well as the consolidation of these variables and their relationships in a conceptual framework that explains insider espionage and serves to predict the associated threats.

To address these objectives, the researcher used a multiple-case analysis method, in which the data from four cases was triangulated through cross-case synthesis. For this purpose, the researcher developed a multidisciplinary conceptual framework consisting of triggers, motives, situational vulnerabilities, markets, and disinhibiting factors. The researcher subsequently performed an in-depth analysis of the constituent elements of these factors. The resulting conceptual framework served as a basis for a multiple-case analysis.

The cross-case synthesis performed in this study supports the view that the five factors precede acts of espionage and can be used to predict associated vulnerabilities. However, the application of the conceptual framework necessitates a complete understanding of the constituent elements. Existing approaches fail to offer this comprehensive view. Based on this study’s findings, the researcher contends that the developed conceptual framework offers greater transparency with respect to insider espionage and its antecedents and can therefore, lay a foundation for greater protection against insider espionage in the future.

KEY TERMS

Espionage; insider espionage; insider spy; insider threat; spy; agent; handler; controller; counterintelligence; five-factor theory of espionage; intelligence collection; security; crime causation; vulnerability.

ABSTRAKT

Spionage hat Regierungen destabilisiert, nationale Sicherheit und wichtige Infrastrukturen gefährdet, die Wirtschaftskraft von Nationen geschädigt und Leben gekostet. Das Problem, das durch die vorliegende Arbeit angesprochen wird, ist das die Prozesse mit denen Insider-Bedrohungen aufgespürt und abgewendet werden sollen häufig ineffektiv sind, weil die Konzepte die den Prozessen zugrunde liegen unzureichend sind. Die vorliegende Forschung untersucht daher die entscheidenden Variablen, die als Prädiktoren für Insiderspionage in staatlichen, zwischenstaatlichen und industriellen Organisationen dienen können. In dieser Arbeit werden auch die Wechselbeziehung dieser Variablen untersucht und in einem konzeptionellen Rahmen (Modell) erfasst, der einerseits Insiderspionage erklärt und anderseits der Vorhersage möglicher individueller Spionagerisiken dienen soll.

Um diese Ziele zu erreichen, verwendete der Forscher eine Multi-Case-Analysemethode, bei der die Daten von vier Fällen durch Cross-Case-Synthese trianguliert wurden. Zur Vorbereitung dieser Analyse entwickelte der Forscher einen multidisziplinären konzeptionellen Rahmen, der aus fünf Faktoren besteht: Auslöser, Motive, situative Vulnerabilitäten, Märkte und enthemmenden Faktoren. Bei der Entwicklung des konzeptionellen Rahmens führte der Forscher eine eingehende Analyse der variablen Bestandteile dieser Faktoren durch. Das daraus resultierende Konzept diente als Grundlage für die Multi-Case-Analyse.

In der Studie folgte eine Cross-Case-Synthese, die die Auffassung unterstützt, dass die fünf genannten Faktoren generell Spionagehandlungen vorausgehen und daher zur Vorhersage individueller Risiken durch Insiderspionage geeignet sind. Die Anwendung des konzeptionellen Rahmens setzt jedoch ein umfassendes Verständnis der variablen Bestandteile dieser Faktoren und ihrer möglichen Ausprägungen voraus. Bisher veröffentlichte Ansätze bieten diese umfassende Sicht nicht. Basierend auf den Ergebnissen dieser Studie argumentiert der Forscher, dass der entwickelte konzeptionelle Rahmen mehr Transparenz in Bezug auf Insiderspionage und ihren Antezedenten bietet und damit künftig eine Grundlage für einen größeren Schutz vor Insiderspionage bieten kann.

SCHLÜSSELWÖRTER

Spionage; Insider-Spionage; Insider Bedrohung; Spion; Agent; Führungsoffizier; Verbindungsführer Spionageabwehr; Fünf-Faktoren-Theorie der Spionage; Aufklärung; Sicherheit; Ursachen von Kriminalität; Sicherheitsschwachstelle; Vulnerabilität

OPSOMMING

Spioenasie het al in die verlede regerings gedestabiliseer, nasionale sekuriteit bedreig, sleutelinfrastruktuur in gevaar gestel, die ekonomiese mag van nasies ondermyn en lewensverlies veroorsaak. Die probleem wat in hierdie navorsing ondersoek is, is gegrond op die meestal ondoeltreffende prosesse en onderliggende begripsraamwerke wat tans gebruik word om die binnekennis-bedreigings wat aan spioenasie ten grondslag lê, aan die lig te bring. Die doel van die huidige studie was derhalwe om ondersoek in te stel na die kritieke veranderlikes wat as aanduiders van binnekennis-spioenasie in regerings-, interregerings- en nywerheidsorganisasies dien; die onderlinge verband tussen hierdie veranderlikes; en die konsolidering van hierdie veranderlikes en hulle onderlinge verband in ’n begripsraamwerk wat binnekennis-spioenasie verduidelik en die gepaardgaande bedreigings voorspel.

Ten einde hierdie doelwitte te bereik, het die navorser ’n meervoudigegeval-analise uitgevoer deur die data van vier gevalle by wyse van dwarsgeval-sintese te trianguleer. Die navorser het vir hierdie doel ’n multidissiplinêre begripsraamwerk, bestaande uit snellers (*triggers*), motiewe, situasionele swakhede (*situational vulnerabilities*), markte en ontinhiberende faktore (*disinhibiting factors*), opgestel. Die navorser het vervolgens ’n omvattende analise van die onderliggende elemente van hierdie faktore gedoen. Die gevolglike begripsraamwerk het as grondslag vir die meervoudigegeval-analise gedien.

Die dwarsgeval-sintese wat uitgevoer is, ondersteun die siening dat die vyf faktore spioenasiehandelinge voorafgaan en gebruik kan word om gepaardgaande areas van kwesbaarheid te voorspel. Die toepassing van die begripsraamwerk vereis diepgaande insig in die onderliggende elemente van die faktore. Bestaande benaderings bied nie hierdie omvattende beskouing nie. Die navorser voer op grond van die bevindings van die studie aan dat die opgestelde begripsraamwerk ’n groter mate van deursigtigheid bied ten opsigte van binnekennis-spioenasie en die omstandighede wat dit voorafgaan en gevolglik die grondslag vir groter beskerming teen binnekennis-spioenasie in die toekoms kan lê.

HOOFTERME

Spioenasie; binnekennis-spioenasie; binnekennis-spioen; binnekennis-bedreiging; spioen; agent; hanteerder; opsigter; kontraspioenasie; vyffaktorteorie van spioenasie; inwin van intelligensie; sekuriteit; veroorsaking van misdaad; kwesbaarheid/swakheid.

SETSOPOLWA

Bohlodi bo dirile gore mebušo e fokole, bo beile tšhireletšego ya setšhaba kotsing, bo beile mananeokgoparara a bohlokwa kotsing, bo fokoditše maatla a ikonomi a ditšhaba le go ama maphelo gampe. Bothata bjo bo rarollwago ka nyakišišo ye bo lebantše go ditshepetšo tšeo gantši di sa šomego gabotse le diforeimiweke tša dikgopolo tša motheo tšeo ga bjale di šomišwago go utulla matšhošetši a ka gare ao a tsopotšwego ka mo godimo ao a lego gona ka gare ga bohlodi. Ka fao, maikemišetšo a nyakišišo ya bjale ke go lekola diphetogo tše bohlokwa tšeo di šomago bjalo ka dihlathollo tša bohlodi tša ka gare ka mekgatlong ya mmušo, ya magareng ga mebušo, le ya intasteri; go amana ga diphetogo tše; gammogo le go kgoboketšwa ga diphetogo tše le dikamano tša tšona ka gare ga foreimiweke ya kgopolo yeo e hlalošago bohlodi bja ka gare le go šoma go bonelapele matšhošetši ao a bolelwago.

Go šogana le maikemišetšo a, monyakišiši o šomišitše mokgwa wa tshekatsheko ya ditiragalo tše ntši, woo go wona datha go tšwa go ditiragalo tše nne e arogantšwe ka motswako wa papišo ya ditiragalo. Go morero wo, monyakišiši o hlamile foreimiweke ya kgopolo ya dikarolo tše dintši yeo e bopilwego ka dihlohleletši, maikemišetšo, go hlaselega gabonolo ga maemo, mebaraka le mabaka ao a thibelago. Ka morago monyakišiši o ile a dira tshekatsheko ye e tseneletšego ya dielemente tšeo di bopago mabaka a. Foreimiweke ya kgopolo yeo e tšweletšego e šomile bjalo ka motheo wa tshekatsheko ya ditiragalo tše ntši.

Motswako wa papišo ya ditiragalo woo o dirilwego ka mo nyakišišong ye o thekga kgopolo ya gore mabaka a mahlano a tla pele ga ditiro tša bohlodi gomme a ka šomišwa go bonelapele mafokodi ao a bolelwago. Le ge go le bjalo, tirišo ya foreimiweke ya kgopolo e nyaka kwešišo ye e feletšego ya dielemente tša karolo. Mekgwa yeo e lego gona e palelwa ke go fa kgopolo ye e feletšego. Go ya ka dikutullo tša nyakišišo ye, monyakišiši o bolela gore foreimiweke ya kgopolo ye e hlamilwego e bea pepeneneng gagolo mabapi le bohlodi bja ka gare le ditiragalo bja yona bja pele gomme ka fao, e ka thea motheo wa tšhireletšo ye kgolo kgahlanong le bohlodi bja ka gare ka moso.

MELAWANA YA BOHLOKWA

Bohlodi; bohlodi bja ka gare; hlodi ya gare; matšhošetši a ka gare; hlodi; etšente; mohentlelara; molaodi wa molao; twantšhotshedimošo; teori ya mabaka a mahlano ya bohlodi; kgoboketšo ya tshedimošo; tšhireletšo; tlholo ya bosenyi; go hlaselega gabonolo

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS USED

ADIV	Algemene Dienst Inlichting en Veiligheid (General Intelligence and Security Service (GISS), Belgium’s intelligence service)
APA	American Psychiatric Association
AU	African Union
BAT	British American Tobacco
BBC	British Broadcasting Corporation
BfV	Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution of the Federal Republic of Germany)
BND	*Bundesnachrichtendienst* (Federal Intelligence Service - foreign and military intelligence agency of the Federal Republic of Germany)
CI	Counterintelligence’
CIA	Central Intelligence Agency
CIL	Customary International Law
COMSEC	Communications Security
COVCOM	Covert Communication
DM	Deutsche Mark
ESA	European Space Agency
EU	European Union
FBI	Federal Bureau of Investigation
FRG	Federal Republic of Germany
FSB	Federal'naya sluzhba bezopasnosti (Federal Security Service - Internal Security of the Russian Federation)
GCHQ	Government Communications Headquarters (United Kingdom)
GDR	German Democratic Republic (East Germany)
GRU	Glawnoje Raswedywatelnoje Uprawlenije (Main Intelligence Directorate of the General Staff of the Armed Forces of former Soviet Union and current Russian Federation)
HVA	Hauptverwaltung Aufklärung (Main Directorate for Reconnaissance of the German Democratic Republic)
ICT	Information and Communication Technology
IGO	Inter-Governmental Organisation
KGB	Komitet Gosudarstvennoy Bezopasnosti (Committee for State Security of the Soviet Union)
LfV	Landesamt für Verfassungsschutz (State Offices for the Protection of the Constitution in the Federal Republic of Germany)

MAD	*Militärischer Abschirmdienst* (Military Counterintelligence Service counterintelligence within the Armed Forces of the Federal Republic of Germany)
MfS	*Ministerium für Staatssicherheit* (Ministry of State Security of the former German Democratic Republic)
MI16	British Scientific Intelligence
MI5	Security Service (United Kingdom)
MI6	Secret Intelligence Service (United Kingdom)
MICE	Money, Ideology, Compromise, and Ego
MIVD	Militaire Inlichtingen en Veiligheidsdienst (Dutch Military Intelligence and Security Service)
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
NATO	North Atlantic Treaty Organization
NSA	National Security Agency (United States of America)
OPCW	Organization for the Prohibition of Chemical Weapons
OPSEC	Operations Security
PERSEREC	Defense Personnel and Security Center (of the USA)
RAF	Royal Air Force
SVR	*Sluzhba Vneshney Razvedki* (Foreign civilian intelligence agency of the Russian Federation)
UK	United Kingdom
UN	United Nations
USA	United States of America
USSR	Union of Soviet Socialist Republics
WTO	World Trade Organization

CHAPTER 1: GENERAL INTRODUCTION TO INSIDER ESPIONAGE IN THE GOVERNMENT AND PRIVATE SECTOR

1.1 INTRODUCTION

Espionage is a sinister crime that occurs in the shadows. Typically, unknown to its targets, espionage has destabilised governments, jeopardised national security, endangered infrastructures, diminished the economic strength of nations, and cost lives (Sale, 2003:3-5; Security Service MI5, 2019:n.p.; Senate Select Committee on Intelligence, 1994:61). The damage inflicted on nations through espionage can be enormous and the penalties for such transgressions often reflect this. Klaus Kuron, a high-ranking counterintelligence officer with the West German Federal Office for the Protection of the Constitution (BfV - *Bundesamt für Verfassungsschutz*) was sentenced to twelve years in prison and fined Deutsche Mark (DM) 692,000 following his conviction of spying for (the former) East Germany for eight years (Bachner, 2018:n.p.). Geoffrey Arthur Prime, a British national who worked as a Russian linguist for the Royal Air Force (RAF) and later for Britain's signals intelligence agency, the Government Communications Headquarters (GCHQ) - the United Kingdom' (UK's)'s signals intelligence agency - was sentenced to 38 years in prison following his conviction on spying for a foreign government for more than 15 years (Osnos, 1982:n.p.).

John Anthony Walker Jr. was a Chief Warrant Officer and communications specialist in the United States Navy. Walker was sentenced to seventeen years in prison for espionage. His brother, Arthur - a retired naval commander - and John Walker's 22-year-old son, Michael - an active-duty seaman - respectively received more than three life sentences and 25 years imprisonment for their spying activities. Jerry Whitworth, who was the fourth member of the Walker spy ring, a Senior Chief Petty Officer and radioman was arrested and sentenced to a 365-year imprisonment term and fined $410,000 for his involvement in the Walker spy ring (Prados, 2014:n.p.).

Espionage was a prolific enterprise during the Cold War era. However, this insidious practice has transcended that era and manifests in more sophisticated forms in the present. Since 1991, there have been many espionage cases, often involving the former Cold War nations, but sometimes also involving new actors (Defense

Personnel Security Research Center, 2009:xii). National law enforcement and security agencies, therefore, are continuously mandated with the development and implementation of effective counter-espionage programmes (Bundesamt für Verfassungsschutz, 2017:n.p.; Federal Bureau of Investigation, 2019:n.p.; Royal Canadian Mounted Police, 2018:n.p.; Security Service MI5, 2019:n.p.).

One noteworthy development in the field of espionage is related to the types of organisations that are being targeted. While the focus of Cold War espionage activities was primarily on political and military targets, the post-Cold-War era has seen a considerable increase in the targeting of corporations and other organisations in the private sector. The instigators are often foreign intelligence services, but corporate competitors are also involved. The accusations against British American Tobacco (BAT) that the company had instigated industrial espionage against its rival cigarette manufacturers in South Africa offer a case in point (Connett, 2016:n.p., Rowell & Aviram, 2019,n.p., Snyckers, 2021:n.p.).

1.2 RESEARCH PROBLEM

The purpose of problem statements is to offer readers an understanding of the issues the researcher intends to address, and to provide arguments that explain the research-worthiness of the issues (Creswell & Poth, 2018:130). While the sources of a research problem may vary, Creswell and Poth (2018:130) suggest that the problem itself originates in some real-life issue, gap in literature or both.

1.2.1 Contextualisation

Creswell (2014:108) emphasises that there are often several issues that establish the importance of a research problem and failing to address these issues leaves it to the reader to decide the importance thereof. Therefore, it is important to contextualise the problem and its attendant issues. The researcher suggests that there are four contextual issues that profoundly illustrate the problem of insider espionage: 1) the damage caused by espionage, 2) the proliferation of espionage, 3) the omnipresence of espionage, and 4) the inadequacy of current policies, procedures, and conceptual frameworks related to insider espionage. These four contextual issues are elaborated in the ensuing discussions.

The principal activities of foreign intelligence services are premised on stealing their targets' most important secrets. In doing so, they may cause substantial personal and material damage at the national level. The unmasking of the espionage activities of Günter Guillaume, an East German intelligence agent who infiltrated the highest echelons of West Germany's government and became Secretary to the West German Chancellor Willi Brandt, destabilised the West German government for weeks. This intelligence scandal eventually caused the resignation of the embattled West German Chancellor (Der Spiegel, 1988:14).

In another incident, the Soviet General, Dmitri Polyakov proffered knowledge to the United States of America (USA) regarding the rift in Sino-Soviet relations, which played a crucial role in United States (US) President Richard Nixon's carving of diplomatic relations with China in 1972 - thereby causing a widening schism in Sino-Soviet relations for decades (Shannon, 2001:n.p.).

Aldrich Ames was an intelligence officer with the Central Intelligence Agency (CIA) who provided the Soviets with information on individuals spying on the Soviet Committee for State Security (KGB - *Komitet Gosudarstvennoy Bezopasnosti)* and the Soviet military. His betrayal caused more than 100 intelligence operations to be terminated, with at least ten CIA agents executed by Soviet authorities (Senate Select Committee on Intelligence, 1994:n.p.).

The post-Cold War era has been characterised by the realignment of espionage, rather than its demise. In 2008, the chief of the Estonian Defence Ministry's security department, Herman Simm, was arrested for providing the Russian Federation's foreign intelligence service - the Sluzhba Vneshney Razvedki Rossiyskoy Federatsii (SVR) - with information on North Atlantic Treaty Organization (NATO) secrets and vulnerabilities of Western cyber-systems. Three years after his arrest, Estonia became the target of a barrage of cyberattacks that lasted three weeks and practically shut the country down (Schmid & Ulrich, 2010:n.p.).

Espionage does not only affect governmental and military institutions. It also impacts commercial, industrial, and academic organisations. The economic damages caused by the theft of intellectual property, trade secrets and knowledge of technological developments, translates into billions of Euros (trillions of South

African Rand) every year (Bundesamt für Verfassungsschutz, 2017; Director of National Intelligence, 2019:n.p.).

Espionage is not an isolated event, as demonstrated in a 2017 report by the US Defense Personnel and Security Center (PERSEREC) listing more than 200 cases of insider espionage – 67 of them since 1990 (Herbig, 2017:B1-9). A recent British Broadcasting Corporation (BBC) report quotes Russian President Vladimir Putin claiming that Russia has foiled the espionage activities of 465 agents of foreign intelligence services in 2018 alone. The same report states that the Dutch, Czech and Swedish security services have also uncovered numerous cases of espionage in their countries (Rosenberg, 2019:n.p.). The Dutch Military Intelligence and Security Service (MIVD) and Britain's Ministry of Justice identified four General Staff of the Armed Forces of the Russian Federation (GRU - *Glawnoje Raswedywatelnoje Uprawlenije*) operatives who were caught trying to hack the computers of the Organization for the Prohibition of Chemical Weapons (OPCW) (Harding, 2018). Additionally, the names of more than 300 agents working for the Russian GRU have surfaced (Nicholls, Mikhailova & Luhn, 2018).

The geographic spread of espionage is a further point of concern. As described above, numerous cases of espionage have emerged in North America and Europe (Herbig, 2017:B1; Rosenberg, 2019:n.p.), and Africa is not unscathed in this regard. A series of documents from global intelligence agencies, known as the 'Spy Cables', were leaked in 2015. These documents harrowingly portray Africa as an emerging '21st century theatre of espionage', with South Africa as the gateway and frequent target of foreign espionage activities (Milne & MacAskill, 2015:n.p.).

In almost all cases of unmasked spies, the discovery of the individual's espionage activity was not the result of successful detection, but of revelations drawn from the information provided by defectors from the side of the opposition (Charney, 2014:19). Individuals whose work involves the handling of classified or otherwise privileged information typically undergo screening (vetting) processes before, and reinvestigations during their employment. These processes, however, often prove to be inadequate. In many instances, individuals with questionable backgrounds are cleared to perform tasks that provide them access to privileged or sensitive information (Olson, 2019:73). Approximately half of the insider spies considered in one study were involved in espionage for a year or more. Routine security screening proved to be ineffective in these cases (Herbig, 2017:29).

Since the processes and underlying conceptual frameworks currently used to ferret out insider threats do not appear to be very successful, the solution suggested by Olson (2019:78) is the more frequent use of rigorous ‘full-scope’ (lifestyle) polygraph tests on a periodic basis. According to Olson, these tests are meant to be aggressive, intrusive, and confrontational; thus, serving as a considerable warning to anyone who might contemplate becoming a spy (Olson, 2019:76).

Charney (2014:19) objects to an emphasis of deterrence as part of a counter-espionage policy. He argues that, if deterrence were an effective instrument, it is difficult to fathom why ‘there never seems to be a shortage of new spies’ (Charney, 2019:22). While polygraph tests have been successfully used in the identification of some individuals involved in espionage, as in the cases of CIA traitors Sharon Scranage and Harold James Nicholson, these tests have also failed, as in the case of Aldrich Ames, who passed routine screening despite his espionage activities (Olson, 2019:76-77).

In addressing the limited effectiveness of current vetting and detection processes, Charney (2019:1) suggests that the problem of insider espionage could be more effectively handled if the intelligence community had a comprehensive understanding of the requirements that must be satisfied (i.e. predictors) for insider espionage to occur. As a psychiatrist, Charney’s focus is on the psychology of spies. He also asserts that the application of other disciplines (e.g., business administration, economics, and mathematics (game theory)) could help in gaining better insight on espionage predictors, which are currently almost all absent from the discussion (Charney, 2019:18-22).

1.2.2 Statement of the problem

The problem addressed through this research project premises on the ineffective processes and underlying conceptual frameworks currently used to ferret out insider threats (Olson, 2019:78). This is a major shortcoming that jeopardises national and corporate security. The foregoing contextual discussion provides the rationale for creating such a conceptual framework. Insider espionage can have devastating material and personal consequences. Cases of espionage occur often enough to constitute a national concern, given also that they occur in secrecy and are difficult to isolate. Furthermore, current policies, processes and conceptual frameworks intended to avert and explain insider espionage have so far been inadequate (Charney, 2019:18-22; Olson, 2019:78). The present research, therefore, sets out to explore the crucial variables that act as predictors of insider espionage in governmental, intergovernmental, and industrial organisations.

1.3 LITERATURE REVIEW

Adler and Clark (2011:89) have defined literature review as 'the process of searching for, reading, summarising, and synthesising existing work on a topic or the resulting written summary of the search'. According to Creswell and Creswell (2018:67), the literature review is a tool with which the researcher summarises studies, as well as conceptual and opinion articles that are relevant to his or her research and offer frameworks for thinking about the topic. For this study, the literature review is categorised into twelve sub-sections. The first subsection provides general observations regarding the current state of intelligence studies literature and the associated challenges, which is followed by a discussion on the evolution of espionage since the earliest known cases in history. This then lays a foundation to address several recent societal developments that have impacted the world of espionage. Globalisation is one such development, which has caused corporate, governmental, and international organisations to become the targets of insider espionage more frequently and with greater ease. Information and Communication Technology (ICT) is another important societal development which has impacted insider espionage. Collectively, both globalisation and ICT demarcate and contextualise the subject of this research most effectively. Sub-sections 1.3.7 to 1.3.12 review and introduce approaches that have emerged during the past three decades which aim to explain and predict insider espionage. The final sub-section addresses the deficiencies in current literature with respect to insider espionage.

1.3.1 The current state of intelligence literature

Intelligence is 'that [which] states do in secret to support their efforts to mitigate, influence, or merely understand other nations (or various enemies) that could harm them' (Warner, 2007:17). Evident in this assertion is that intelligence provides the sources and the means that enable governments to understand the inner workings of other nations and to exercise influence on them. Since other nations often resist such activities, intelligence is fragile and frequently subject to loss of its sources and means. For this reason, its practitioners treat intelligence as something that is sensitive and confidential (Warner, 2007:17).

According to Warner (2007:17), intelligence resists scholarship because of the sensitivity and confidentiality associated with it. It is therefore not one field of study but two. One is on the 'outside' that only has access to public documents and therefore studies the various phenomena in much the same way that historians study history. The other is on the 'inside' with access to the most sensitive records but with limited scholarly inquiry. Despite this dichotomy, methods in both worlds, the outside and the inside, have brought practitioners and researchers closer to a genuine understanding of phenomena related to the field of intelligence (Warner, 2007:17).

May (1995:1) asserts that when intelligence studies emerged as a field of scholarly inquiry, the body of available literature was at or below that of the field of business education when it emerged. It was only from 1975 onwards that the number of publications on intelligence-related subjects slowly began to grow. In a field as broad as intelligence, only 100 of the 914 (11%) intelligence-related articles published in the 'Intelligence and National Security' journal between 1986 and 2011) were related to the field of counterintelligence, and only a subset of those were focussed on espionage. However, despite the relative novelty of intelligence as a field of research, the body of scholarly literature in this field is growing, which allows academic training and further research to evolve (Johnson, 2014:10-12).

Warner (2007:22) suggests that the inquiry of researchers working on intelligence from the 'outside' resembles that of researchers studying history. Their work relies heavily on literary sources. For intelligence scholars, this means identifying all official documents, studies, and reports available in the public domain. Declassified documents offer particularly valuable insights. News reports present a further source of data for intelligence scholars. While such reports may be fragmentary and contain inaccuracies, they are also very much used for intelligence research both inside and outside the intelligence community. Memoirs, autobiographies, and biographies also provide a further source of data for scholarly inquiry (Warner, 2007:22-23).

1.3.2 The evolution of espionage through the ages

Espionage is a phenomenon that is almost as old as civilization itself and reflecting on its history is important for a variety of reasons. Clearly, historic reflections provide a foundation and context on the subject. Such reflections also exemplify how the *zeitgeist* of a society and the concerns of the leaders of a people determine the targets of espionage and the type of information that is sought through it. Historic reflections on espionage also highlight how technological developments, most recently those in the field of information and communications technology (ICT) and the advent of the internet, have affected the espionage tradecraft and ultimately facilitated espionage. In this regard, developing an understanding of the origins and the evolution that espionage has undergone to this day, makes it possible to predict its future.

The earliest known accounts of the use of espionage for strategic advantages date back to the era of King Hammurabi of Babylon whose reign lasted from c. 1792 BC to c. 1750 BC (Sheldon, 1989:9). In the 1760s BC, Hammurabi waged war against Elam and the city states of Eshnunna and Larsa. Faced with the challenge of devising a successful military strategy, Hammurabi demanded information about the enemy's strength, position, and intentions. In a letter to Zimri-Lim (Ruler of Mari and Hammurabi's war ally), Hammurabi wrote: 'I will not send (troops) as long as I do not have information concerning the enemy' (Sheldon, 1989:9). To an emissary of Zimri-Lim, Hammurabi wrote: 'Let [a messenger] remain for (at least) five days until we see complete information concerning the enemy' (Sheldon, 1989:9). Equipped with the information he required, Hammurabi was then able to formulate a military strategy with which he would finally defeat the enemy forces (Sheldon, 1989:9).

Since ancient times, espionage has been used to gather intelligence regarding opposing military forces and also on the civilian population of foreign nations and the resources they possess. The Book of Numbers (attributed to the 13th century BC) narrates events concerning Moses leading the Israelites from Egyptian oppression to freedom in Canaan. Moses sent out twelve spies to gather information in advance of the invasion by traversing the Negev desert and entering the hill country. From there, they were to assess the kind of land that the Canaanites lived in, the size of their population, and whether the Canaanites were strong or weak. The spies were also to determine the kind of towns the Canaanites inhabited, and whether their towns were unwalled or fortified, whether their soil was fertile or poor, and whether there were trees on their land or not (New International Version, Num. 13:3-20). While the historicity of this account has been the topic of much scholarly debate (Collins, 2005:45), it is undeniable that the account itself is ancient, and thus, that the notion of using espionage to support a strategy that goes beyond military considerations already existed then.

Historically, espionage has also been used to collect economic and political information. For instance, from the 7th century B.C., Carthage gradually expanded its economic and political influence across the Western Mediterranean through a variety of military campaigns, the reinforcement of its trade routes, and the founding of new colonies. Before embarking on a military campaign, the Carthaginians carefully explored remote coastal regions, examined the economic prospects and political integrity of potential target areas, and thus gathered considerable strategic knowledge. It was on the basis of this knowledge that the Carthaginians set their objectives. The battles of Alalia, Selinus, and Himera are examples of Carthaginian use of intelligence gathering to select economically promising targets and prepare for invasions. Around 530 BC, the Carthaginians and Etruscans took control of Corsica in the Battle of Alalia and succeeded in expelling the Greeks from this island.

Around 410 BC and 409 BC, the Carthaginians launched invasions against the cities of Selinus and Himera on the island of Sicily. They defeated the armies, captured the former and obliterated the latter of the two cities (Barceló, 2003:30). Since the strategic objective of the Carthaginians was to expand their economic and political influence, the military campaigns were essentially the means through which they achieved these goals. It is noteworthy that for the Carthaginians, espionage was instrumental not only in supporting their military strategies, but also their political and economic objectives (Barceló, 2003:30-31).

For centuries before the Industrial Revolution around 1700, nations largely relied on their agricultural capabilities to achieve wealth. However, as new technologies and improved production methods were developed, industrialisation took hold, factories were established, and new sources of wealth emerged (Beck, Black, Naylor & Ibo Shabaka, 1999:634-635). Entrepreneurs needed money, machinery, and manpower to produce their goods, as well as the knowledge of production processes with which their goods could be manufactured (Beck et al., 1999:634-635).

It was during the early Industrial Revolution that economic espionage was no longer used only to identify the lands that could be seized to gain greater wealth, but also to purloin other nations' production and manufacturing secrets to advance the spying nation's own economy. During the Ming Dynasty (1368–1644 AD), porcelain became a commodity that was valued well beyond the borders of China. Imported by merchants travelling via the Silk Road, Chinese porcelain had become, and remained a prized possession indicating wealth and status throughout Asia, Africa, and Europe for centuries. The admiration for Chinese porcelain was so great that potters in the West who sensed an opportunity to achieve great riches, often tried but failed to imitate the porcelain production process (Kleiner, 2016:1053).

The porcelain manufacturing efforts of the German alchemist, Johann Friedrich Böttger were finally successful and resulted in establishment of the Meissen Porcelain Manufactory in 1710 (Staatliche Porzellan-Manufaktur Meissen, 2021:n.p.). Unaware of this development in Germany, the French Jesuit priest, François Xavier d'Entrecolles (who was a missionary in China), used his contacts with converted Chinese locals to gain knowledge of the porcelain manufacturing process. He detailed his findings in a letter he sent to Father Louis-François Orry in Paris in 1712. Father Orry, who was the treasurer of the Jesuit missions to China and India at the time, disseminated d'Entrecolles' findings in the Jesuit missions' annual report. Equipped with d'Entrecolles' detailed letter and samples, it became possible to produce porcelain in France. This eventually led to the establishment of the Manufacture Nationale de Sèvres in 1740, which still exists to date and became a precursor to the decline of Western interest in Chinese porcelain (Hillier, 1968:190-192).

While the scope of information sought through espionage may have broadened over time, now encompassing military, political, economic, and industrial intelligence, the resources with which espionage was conducted remained largely unchanged. Governments typically continued to maintain rather small organisations whose task it was to collect intelligence. Underfunded and understaffed, these organisations typically existed at the periphery of their governments with little direct access to their top leadership (Richelson, 1995:5). In the first half of the nineteenth century, most of the intelligence used by heads of state or heads of government was not provided by these organisations, but by foreign-based attachés who gathered information in their host countries. It was common for the gathering of information by attachés to be constrained by prevailing notions of ethical conduct and expected to occur in a 'gentlemanly and honorable fashion' (Richelson, 1995:5). Attachés were discouraged from stealing secrets and were only to collect information that was readily and openly available (Richelson, 1995:5). To this effect, Furgusson (1984:212) quotes a British attaché of the time as stating:

> 'I would never do any secret service work. My view is that the military attaché is the guest of the country to which he is accredited and must only see and learn that which is permissible for a guest to investigate. Certainly, he must keep his eyes and ears open and miss nothing, but secret service is not his business, and he should always refuse a hand in it' (Richelson, 1995:5).

The late 19th century brought about considerable changes in this regard. With tensions growing between nations, the heads of state and heads of government became increasingly anxious about the intentions and activities of their rival states. They were also less concerned about the ethics of acquiring secrets, which led to the creation of larger intelligence gathering organisations as well as an increase in funding for intelligence activities. In 1863, Italy established the *Ufficio de Informazione* (Office of Information) under the High Command of the Italian Army. Three years later, just days before the outbreak of hostilities between Prussia and Austria, Germany established the *Politische Feldpolizei* (Political Field Police). Both organisations (Office of Information and Political Field Police) were established to gather secret information about military adversaries (Richelson, 1988:102).

A year after its crushing defeat in the Franco-Prussian War of 1870, France established the Deuxième Bureau as part of its General Staff of the Armed Forces. Within the Deuxième Bureau, the Section de Statistique (Statistics Section), which was later renamed the Service de Renseignements (SR, Information Service), had the task of gathering intelligence on German troop movements (Richelson, 1995:7). Great Britain established the Intelligence Branch within its War Office in 1873, and the British Admiralty organised the Foreign Intelligence Committee in 1882, which it renamed Naval Intelligence Department in 1887 (Richelson, 1995:7). In the years that followed, more intelligence organisations emerged across the globe. By the late 1800s, most major and middle-ranking powers had established their own intelligence organisations (Richelson, 1988:1-2).

The early 20th century was marked by growing tensions between nations globally. Military expenditures that had been rather stable over time were now reaching unprecedented levels. Compared with the level of standing army personnel among the so-called great powers (i.e. Germany, Austria-Hungary, Italy, British Empire, France, and Russia) in 1890, the level had steadily grown by 64% by 1914. During the same period, army appropriations among these countries had grown by 140%. Naval tonnage had climbed by 360% and naval appropriations had risen by 285% (Black & Helmreich, 1972:27). The profound growth in volume, complexity, and diversity of military resources required a greater effort in collecting information about the developments in rival countries.

Intelligence collection, however, has been hampered by the primitive state of development within the intelligence organisations that often depended on information from unreliable sources. This circumstance necessitated an increase in the number of intelligence personnel and their professionalism, but also in the technologies they used (Richelson, 1988:1-2). Facilitated by the Russian Revolution, both the First and Second World Wars, the Cold War, and numerous other national and international conflicts, intelligence agencies went from small organisations with not more than a few hundred personnel prior to the First World War, to becoming large organisations with thousands of employees and complex responsibilities, capabilities, and competencies in the world today (Richelson, 1988:3).

1.3.3 The impact of globalisation on espionage

Throughout most of the 20th century, nations were typically either aligned or at odds with each other, connected with or disconnected from each other, along the lines of their political interests and ideologies. Political, economic, and cultural interactions took place on a global level, but their focus was limited to partner nations that were politically and ideologically aligned (Schaeffer, 1997:22-24; Shiraz, 2017:265). Throughout the 1990s, post-Cold War realities engendered a new *zeitgeist* and a 'meteoric rise of public interest in globalisation' (Eriksen, 2014:3), which meant a move towards greater integration and interdependence of nations across numerous dimensions (Herbig, 2017:152). With the concept of globalisation came the widespread sense that the world was being compressed and that public consciousness of the world as a whole was being intensified (Robertson, 1992:8).

In a spirit of great optimism, nations that previously had adversarial relations were now actively seeking closer cooperation with each other (Eriksen, 2014:123). Interests that were previously addressed at a national or regional level, or with select partners (e.g., for climate change and space exploration), were now being addressed with broader participation. In a rapidly changing world, globalisation became 'the expansion of a global political system, and its institutions, in which inter-regional transactions (including, but certainly not limited to trade) are managed' (Thompson, 2008:59). It was in this spirit, that inter-governmental organisations gained further prominence.

Driven by economic and technological developments, distances in a globalised world have become irrelevant or at least less important than they have been in the past. The speed of communication and transportation of goods and commodities has reached levels that were unimaginable only a decade before. Furthermore, inexpensive plane tickets, cheap calls, and perhaps most importantly, the internet, are some of the factors that have contributed to integrating the world (Eriksen, 2014:8). Globalisation has widened the field of interrelationships to include nations that had been largely excluded from trade relations in the past, and it opened markets that had formerly been inaccessible. Globalisation has also provided the impetus to focus on creative processes and innovative ideas that could be leveraged with a view to enhancing greater participation in this changed environment (Herbig, 2017:171).

Culturally, globalisation has manifested itself through an increased exchange in spheres such as music, television, cinema, and tourism. The cultural lines that had previously separated nations from one another throughout history, now appeared increasingly blurred and immaterial (Beynon & Dunkerley, 2000:18; Herbig, 2017:171). Politically, the world appeared to be moving away from the narrow focus on national interests towards an emphasis on humankind and global responsibility (Robertson, 1992:27-28). For many institutions and organisations, the notion of global citizenship took precedence over that of national citizenship. The institutional emphasis on global citizenship had become immanent in educational curricula, conferences, and organisations, and among spokespersons; all of which are devoted to upholding the notion of global citizenship. Reflecting on the newly emerged *zeitgeist*, Israel (2012:n.p.) suggested that '… as a result of living in a globalized world, we understand that we have an added layer of responsibility; we also are responsible for being members of a world-wide community of people who share the same global identity that we have' (Israel, 2012:n.p.).

Throughout the 1990s, globalisation was primarily seen as an expression of greater understanding between nations and as an instrument to improve international relations. However, in the 2000s, it became increasingly evident that globalisation could also have negative influences (Eriksen, 2014:123). For instance, criminal networks were progressively operating 'in both legal and illegal sectors, depending on what [could bring] them the greatest benefit' and transnational organised crime had become an inherent feature of globalisation (Heinrich-Böll-Stiftung & Schönenberg, 2013:11). Globalisation also came to be regarded as a main driver of transnational radicalisation among members of extremist religious and nativist groups (Kaya, 2021:204). The 9/11 attacks on the World Trade Center in New York City and the Pentagon in Arlington, Virginia, raised public awareness regarding the globalisation of terrorism as well (Eriksen, 2014:123). Consequently, the optimism associated with globalisation throughout the 1990s had to some extent, given way to a public sense of fear and foreboding. Globalisation was no longer seen as an instrument of transnational understanding and collaboration, but also as a volatile, anarchic, and dangerous state that was associated with a loss of control (Eriksen, 2014:123).

One of the features of globalisation is that it de-emphasises the importance of the individual nation, which can prompt a reduction in an individual’s exclusive commitment of allegiance to a single nation, cause loyalties to be divided, and possibly entirely replace national allegiance with an allegiance to global citizenship (Herbig, 2017:56). It can cause individuals to imagine that by helping another country, they are acting on a higher moral plane (Herbig, 2017:56). This is an important consideration because of the frequency and trend with which it occurs. According to a study covering the 68-year period from 1947 to 2015, money has always been the most frequent motive of espionage, followed by divided loyalties as the second most frequent motive. However, while the post-Cold War frequency of financially motivated espionage decreased by 37%, the frequency of espionage based on divided loyalties has increased by 57%. This development means that the frequencies of the two motives are convergent, and that divided loyalties are beginning to rival the financial motive (Herbig, 2017:46 & 51).

Globalisation has also had an effect on the range of espionage targets. The continued ‘integration of markets, nation-states, and technologies’ has enabled the world to ‘reach farther, faster, deeper, cheaper than ever before’ (Fink, 2002:12). Such a reach has engendered the development of new opportunities for international cooperation between governments, corporations, and universities, but also opened new opportunities for insider espionage. Intergovernmental organisations, created to equally serve the interests of all their member states, have become ‘regular hotbeds of intelligence gathering’ (Gowan, 2018:n.p.). As a factor of globalisation, an increase in economic and industrial espionage has occurred, instigated by both corporate competitors and governments that regard industrial espionage as a means to equalise international market competition (Fink, 2002:12). Similarly, universities and other research establishments have become the targets of insider espionage, particularly those involved in the development of prized technologies (Bundesamt für Verfassungsschutz, 2021:n.p.).

1.3.4 Espionage in the private sector

Historically, espionage has targeted, and continues to target military and governmental institutions (Barceló, 2003:30-31; Gowan, 2018:n.p.; Sheldon, 1989:9). More recently, however, espionage efforts have also been directed toward the collection of information in the private sector (Hillier, 1968:190-192; Fink, 2002:12; Bundesamt für Verfassungsschutz, 2021:n.p.). The latter development raises the question of whether approaches that have been developed with a view to insider espionage in the public sector also apply to targets in the private sector (i.e. corporations, private research institutes, universities).

According to Benny (2014:8-10), Geis (1994:127) and Wimmer (2015:14-16), offenders found guilty of insider espionage in the private sector have typically been driven by the same motives as those in the public sector. While this claim seems plausible and supported by a PERSEREC study, the sample size of industrial insider spies (n=21) and the geographic scope of the study (USA only) hardly allows for global generalisations (Defense Personnel Security Research Center, 2009:xiv).

The customers of stolen trade secrets fall into two broad categories: foreign intelligence agencies and corporate competitors. Foreign intelligence agencies engage in industrial espionage to aid their countries' economies, enable their domestic industry to gain a competitive edge, and support their nation's domestic agenda. This poses a particular risk to the targeted private sector because of the professionalism with which information gathering is organised by foreign intelligence agencies, and because security programmes in the private sector often present no effective match for the information collection capabilities of these agencies (Benny, 2014:10).

The tradecraft used by foreign intelligence agencies involved in industrial espionage typically follows the same pattern as that used in espionage activities against governmental and military targets. Recruitment and exploitation of assets follow the same procedures (Benny, 2014:19-23) and the intelligence cycle (consisting of planning and directing information gathering activities, collecting, processing, and analysing the stolen information, and disseminating the final intelligence products) is applied as much to information stolen from private sector targets as from governmental targets (Tsolkas & Wimmer, 2013:9; Benny, 2014:17-19).

Similar to foreign intelligence agencies, corporate competitors can pose a substantial espionage threat to the private sector. While much of the information collected by corporate competitors is publicly available and gathered as legal open-source intelligence (OSINT), there have been numerous instances in which employees of a company have volunteered trade secrets to a competitor who has gratefully accepted the information in exchange for a reward. In addition, there have also been instances of the corporate actor initiating the espionage activities, targeting specific types of competitor information, and structuring operations similar to those of foreign intelligence agencies (Benny, 2014:11-12).

1.3.5 Espionage in international organisations

Similar to organisations in the private sector, international organisations (intergovernmental organisations) have become favoured targets of insider espionage. Intergovernmental organisations (IGOs) are entities 'created by treaty, involving two or more nations, to work in good faith, on issues of common interest' (Harvard Law School, 2019:n.p.). Their main purpose is to provide a framework of cooperation in the areas of peace and security, but also with respect to a host of other issues like economics, social welfare, science, and technology. Inter-governmental organisations are numerous in number, and include the United Nations (UN), the North Atlantic Treaty Organization (NATO), the African Union (AU), the Association of Southeast Asian Nations (ASEAN), the European Union (EU), the Organization of Petroleum Exporting Countries (OPEC), and the World Trade Organization (WTO) (Harvard Law School, 2019:n.p.; United Nations Convention Against Transnational Organized Crime, 2010:n.p.).

While international organisations emphasise their contributions to the interests of all their member states, they are also frequently the site of insider espionage. United Nations officials have been quoted as stating that 'any or all rooms in their headquarters in New York could be tapped' (Gowan, 2018:n.p.). On many occasions, agents have been known to plant themselves in translation booths to follow developments during UN meetings, thereby collecting information that they could pass on to their principals (Bosco, 2012:n.p.).

Espionage in international organisations is widespread, and benefits from customary international law (CIL), which weakens State accountability (Navarrete & Buchan, 2019:897). Moreover, staff of international organisations typically enjoy diplomatic or functional immunities protecting them from 'legal process in respect of words spoken or written and all acts performed by them in their official capacity' (Reinisch, 2009:3). This may explain the comparatively few cases of espionage in international organisations coming to light. Notwithstanding, there are a few instances in which such transgressions were considered particularly damaging to merit prosecution. For instance, Rainer Rupp from Germany, Herman Simm from Estonia, and Frederico Carvalhão Gil from Portugal - all NATO insiders - were charged with spying against NATO in 1993, 2008 and 2016 respectively (Sontheimer, 2014:n.p.; Scally, 2008:n.p.; Schindler, 2016:n.p.). More recently, a major in the Belgian General Intelligence and Security Service (ADIV - *Algemene Dienst Inlichting en Veiligheid*) whose identity has so far not been disclosed to the public, has been accused of endangering the European Union through espionage activities (Rettman, 2019:n.p.).

1.3.6 The impact of ICT on espionage

Globalisation has brought people closer together but has also opened new opportunities for perpetrating insider espionage. The development of information technologies has been instrumental in facilitating global convergence and the attendant espionage activities. The field of information technology has undergone significant changes over time and eventually revolutionised information collection, processing, storage, and dissemination. The development of the semi-conductor in the late 1940s and the integrated circuit and metal–oxide–semiconductor field-effect transistor (MOSFET) in the late 1950s has presaged the development of mainframe computers in the 1960s and 1970s. Despite their costs, these mainframes were in high demand by countless large organisations in the public and private sectors because they could handle large amounts of data in hitherto unimaginable ways (Eden, 2018:16; IBM, 2022:n.p.).

Working with mainframes was cumbersome and accessing them was limited to a relatively small population. Notwithstanding, the introduction of the personal computer (PC) in the 1980s rapidly brought about changes in both respects (i.e. limited access and cumbersomeness). It became commonplace for office workers to have computers on their desks, and an ever-increasing number of small businesses and private households were purchasing them as stand-alone units to serve their diverse needs. While it was unusual to find an office workplace that was equipped with a computer in the early 1980s, it eventually became unusual to find an office workplace without one (Eden, 2018:16; IBM, 2022:n.p.).

The introduction of the internet in the 1990s dramatically changed the ease with which information could be gathered and relayed. The internet also enabled users to communicate with one another through their PCs and eventually to gain access to vast amounts of information at the touch of a button (Eden, 2018:16; De Wet, Koekemoer & Nel, 2016:1). The technologies combining information and communications had become inseparable and pioneered what is now known as information and communication technology (ICT). The progressively widespread access to ICT transformed the way in which people thought, interacted, and worked. It soon became evident that ICT was essential for organisations to remain competitive, efficient, and cost-effective. Ultimately, failure to adapt to the new ICT-induced environment that the information age has bestowed upon the world could pose a grave risk to organisational survival (De Wet, Koekemoer & Nel, 2016:1; Müllner & Filatotchev, 2018:91-92). It should also be borne in mind that ICT has affected individuals by opening opportunities for personal cross-border mobility and exchange that was non-existent previously (Müllner & Filatotchev, 2018:92).

In the past four decades, the processing and storage capacities of computers and the range and capability of software applications have continuously grown and ushered-in a steady increase in the amount and variety of data with which computer systems have been populated. These developments have brought about numerous benefits for the organisations involved, and also exposed organisations to a wider range of risks due to the new espionage opportunities they have created (Ferguson, 2004:80; Herbig, 2017:147; Lucas, 2018:12-13; Mehan, 2016:35).

Starting in the 1980s, governmental and private organisations increasingly moved towards the consolidation and centralisation of information technology resources, as well as the consolidation and centralisation of the information contained in these resources. While the centralisation of information, has enabled organisations to achieve greater efficiency, it has also increased the target density and target value in the realm of espionage (Mehan, 2016:75). Most recently, this trend could be witnessed in the use of the cloud and the evolution of big data. Big data has further increased the velocity, variety, and volume of available information. It has magnified the threat of insider espionage because of the large amount of data that can be retrieved from a single source with minimal effort (Mehan, 2016:86).
Information and communication technology has also affected the way in which spies exploit targets by offering further options (Clark, 2014:126-127). Spies may use their own access privileges and also masquerade as other authorised users or exploit human assets (e.g. colleagues) to illegally gain access to computer networks through which they can leave a backdoor behind in order to bypass the network authorisation process during later system penetrations (Clark, 2014:126-127).

Insider spies can now also retrieve masses of data across digital boundaries and bring them into their possession without having to rely on the limited storage capabilities of data media (Mehan, 2016:35). For instance, Ryszard Jerzy Kukliński, a colonel in the Polish army and a spy for NATO during the Cold War, provided his handlers with an impressive 35,000 secret Soviet documents which he amassed between 1972 and 1981 (Weiser, 2004:47-49; Fischer, 2000:25). Today, the same amount of information could be retrieved in a matter of days and could be stored on a memory card the size of a postage stamp. Spies no longer need to use concealment devices for hiding film, one-time pads, or secret writing chemicals. They can use innocuous objects like toys, cameras, digital music players, calculators, watches, automobiles, and home consumer products that contain embedded computer chips which can be altered to contain secret information. By using such everyday objects, the probability of detection is virtually non-existent (Wallace & Melton, 2008:447).

Similar to the computer, the internet has also had a profound effect on espionage in its relatively short time as the single largest source of publicly available information. Through its global system of interconnected computer networks, the internet has made it possible to collect information on almost any subject of interest. While the quality of internet-based material varies greatly and much of the information is misleading or entirely incorrect, there is also a vast amount of information that is accurate and useful. With the necessary precautions, the internet is a valuable tool for the collection of open-source intelligence (Clark, 2014:26). For individuals who intend to offer their services as spies, the internet has become a treasure trove of information. Most spies first establish contact with their future handlers through the embassies of the countries for which they intend to work. All relevant information about these embassies (i.e., their locations and opening hours) can be gathered online in just a few minutes. Moreover, almost all major intelligence services have websites containing their contact information. Upon initial contact, these services are likely to respond, should they believe that the individual is a promising prospect (Ferguson, 2004:236).

The internet has had an effect on all aspects of the intelligence tradecraft. However, none has been affected more than covert communication (COVCOM). Through encryption capabilities, the internet offers unprecedented opportunities for information to flow without exposing the location and identity of the sender or recipient. It also provides ways to conceal all aspects of a communication ‘in a bewildering variety of disguises’ (Wallace & Melton, 2008:448). During the Cold War, COVCOM plans could require weeks of preparation and would still be dangerous to execute. Through the use of the internet, messages can be safely sent in just seconds, their very existence can be masked, and illicit communications can be transmitted with probable impunity. At the same time, the volume of material that can be sent is practically unlimited (Wallace & Melton, 2008:448-449).

In summary, ICT has enabled spies to access privileged information that they otherwise would have had considerable difficulty accessing. ICT has also diminished the levels of risk. The volume of information that spies can now access is greater than it was prior to the advent of ICT. The possibilities for information storage and concealment have made detection almost impossible. The internet has considerably reduced the transaction efforts by providing information about potential customers with the touch of a button. Therefore, the encryption capabilities on the internet have considerably reduced the risk of detection, while also allowing vast amounts of information to be transferred.

1.3.7 Theories of insider espionage causation

In light of the expansion of intelligence collection activities, changes in the *zeitgeist* with respect to globalisation and the evolution of ICT, the need for effective programmes to combat insider espionage is arguably greater than ever before. This is the province of counterintelligence. The term ‘counterintelligence’ (CI) is used to describe the organisations that are tasked with the protection of secrets from foreign acquisition and penetration. The term also refers to the schemes and multidisciplinary efforts that are used to provide security and protect secrets from adversaries (Carlisle, 2005:172, Johnson, 2009:1-3, Prunckun, 2012:23). Richelson (2016:438) suggests that counterintelligence consists of the below-cited six components:

- Investigation aimed at identifying individuals who are operating on behalf of foreign intelligence agencies and security services;
- Collection of information on the activities of foreign intelligence agencies and security services;
- Evaluation of individuals who have defected and prospective agents;
- Development of intelligence products (reports) containing insights into the structure, personnel, and operations of foreign intelligence agencies and security services;
- Disrupting and neutralising activities of foreign intelligence agencies and security services; and
- Provision of support to friendly intelligence services and security services as well as to operational activities (Richelson, 2016:438).

While these components have always been the responsibility of a functioning counterintelligence service, history proves that the effectiveness of counter-intelligence activity has often been lacking. To that effect, Van Cleave (2009:26) argues that:

> The sorry history of successful, long-standing espionage carried out by trusted insiders is an indictment of the ‘each is responsible for its own house’ approach to counterintelligence. Nevertheless, counterintelligence

> (and especially counterespionage) breeds an imperative to hold close to information and to stay in control of these extremely sensitive operations and investigations.

The afore-cited excerpt suggests that counterintelligence has often been neglected and given less attention than intelligence has (Van Cleave, 2009:26). This could partially explain the absence of espionage theories from intelligence literature until this phenomenon could no longer be ignored in the 1980s. In the USA, the number of insider espionage cases known to the public from 1950 until 1974 averaged approximately 9 per year, and a maximum of 16 in 1959 and 1960. From 1975 to 1989, the average increased to approximately 28 per year, with a maximum of 41 in 1984 (Herbig, 2008:44). It was after this development that theories of insider espionage began to emerge in intelligence literature.

According to Eoyang (1994:71-85), theories explaining why individuals become insider spies can be divided into four categories: psychological, situational, situation-dispositional, and behaviour chain (process-oriented) theories. Psychological theories of espionage focus on the individual and essentially address motivation and personality (Eoyang, 1994:71-72). With an emphasis on the detection of espionage rather than its prevention, the psychological paradigm continues to dominate the field of counterintelligence when screening and selecting personnel for security-sensitive positions (Charney, 2019:37).

The field of psychology offers a considerable body of relevant knowledge providing insights into the causes and factors of deviant behaviour, elaborate technologies for testing and measuring human traits, and understanding individuals' personalities, needs, emotions and mental health, as well as the motives and incentives of crime in the case of criminal psychology. With respect to the study of espionage, understanding human traits lays the foundation for a paradigm that is focussed on a specific group of individuals (i.e. insider spies) who are members of a larger population of individuals who have access to sensitive information (Charney, 2019:37; Eoyang, 1994:71).

Situational theories address a range of factors in the environment of individuals who become spies. These may include security, sociological, organisational, and other external factors that affect individuals and cause them to enter the field of espionage

(Eoyang, 1994:78). Situational-disposition theories consider both the propensities of an individual to commit espionage and the environmental contingencies that facilitate or promote this act. Eoyang (1994:78) asserts further that the psychological and the situational theories are each incomplete and, therefore, require complementarity. By synthesising the two approaches into one, it is possible to gain a more comprehensive understanding of reasons for individuals becoming insider spies (Eoyang, 1994:81).

1.3.8 Motivational approaches

Levchenko (1988:106) is credited with being the first to publish a motivational explanation of insider espionage. More recently, Smith (2017:5) has advanced a motivation-based approach to explain why individuals become insider spies. Whenever a case of insider espionage emerges, questions are soon raised concerning the reasons for the spy's treachery.

Stanislav Levchenko was arguably one of the Cold War intelligence officers best positioned to provide an answer in this regard. Levchenko was a major in the Soviet-era KGB and responsible for recruiting and handling its numerous agents in Japan before his own defection to the West in 1979 (Trahair, 2004:166-167). Levchenko (1988:106) asserts that his success as a recruiter was attributable to an American recruitment approach, recognised by intelligence services around the world and used as a measure for determining an individual's vulnerability when persuaded to become an agent of a foreign power. The approach focuses on four possible motives that explain an individual's decision to become an insider spy, namely: money, ideology, compromise, and ego (hence the acronym MICE) (Levchenko, 1988:106).

To this day, intelligence agencies are primarily focussed on motivation in their efforts to unmask spies. The Central Intelligence Agency (CIA) has a branch that is specifically tasked with looking into the psychological motivations of agents and provides psychological assessments in this regard. The Federal Bureau of Investigation (FBI) continues to use the MICE acronym as a framework for its counter-espionage work (Smith, 2017:14). The MICE acronym also continues to be taught in intelligence training and academic intelligence studies programmes today (Burkett, 2013:9; Houben, 2003:269).

Recognising that the focus on motivation is an important standard of intelligence communities when reflecting on the predictors of insider espionage, Smith (2017:14) asserts that focussing on money, ideology, compromise, and ego alone offers a rather narrow perspective. In Smith's view, there are six variables that may act either individually or in concert to motivate an individual's decision to become a spy. These variables are: sexual relationships, money, patriotism, adventurers, fantasists, and psychopaths, revenge, and doing what is right (Smith, 2017:5).

Smith (2017:5) also observes that 'honey traps', 'Romeo-operations' and other variants that leverage a sexual relationship have been so prominent in numerous insider espionage cases, that they warrant a category of their own (i.e. sexual relations) (Smith, 2017:15). In agreement with Levchenko (1988:106), Smith (2017:53-54) regards money as an important incentive citing numerous examples of insider espionage attributable to this factor. However, rather than ideology, Smith alludes to patriotism as a further key motive for insider espionage. He views ideology and patriotism as complementary in that, individuals motivated by one or the other (or both) engage in espionage 'for the good of the cause' (Smith, 2017:95).

Smith's (2017:95) category of adventurers, fantasists and psychopaths addresses a group of individuals whose psychological framework influences the prospect of working in the intelligence field as appealing. However, once employed, they are likelier than others to become dissatisfied with the often-mundane work of an intelligence officer. This makes these individuals susceptible to the recruitment efforts and subsequent espionage activities of foreign intelligence agencies (Smith, 2017:143).

Revenge is 'one of the most powerful and enduring motives of a traitor' (Smith, 2017:183). Such a motive emanates from the anger and indignation of individuals due to experienced or perceived unfair treatment. This motive feeds on itself because each act of betrayal (revenge) reminds the spy of the injustice to which he or she believes to have been subjected (Smith, 2017:183).

Based on his category of ‘doing the right thing’, Smith (2017:221) addresses an important aspect in our understanding of insider spies, who are often characterised as unscrupulous and ruthless individuals who will not be deterred in acquiring what they want. He asserts that this view, however, does not always reflect the realities and cites several cases of insider espionage in which the spy acted for some greater good rather than for selfish reasons (Smith, 2017:221).

Moore, Savinda, Monaco, Moyes, Rousseau, Perl, Cowley, Collins, Cassidy, VanHoudno, Buttles-Valdez, Bauer and Parshall (2016:1) reflect on insider spies’ motives and incentives in a different way. These authors assert that measures aimed at reducing the risks of insider threats are traditionally built on negative incentives, and that the excessive reliance on such practices can, in fact, achieve the opposite and exacerbate insider threats by causing employee disgruntlement. In this sense, such practices may act as triggers. In an approach influenced by the organisational behaviour perspectives, Moore et al. (2016:1-2), suggest that the negative incentives used to mitigate the risk of insider espionage should be complemented with positive incentives. Accordingly, Moore et al. (2016:1-2 & 5), explore three dimensions through which positive incentives could be offered to employees: 1) job engagement, 2) organisational support, and 3) connectedness with co-workers.

In the researcher’s view, motivational approaches to insider espionage are useful as a reminder that espionage as a type of human behaviour is preceded by a variety of motives. It is also helpful to explore the specific incentives that have prompted individuals to become spies. These approaches, however, are also replete with several shortcomings. Firstly, they narrowly focus on only one factor: the motive. While it is undisputed that a motive precedes insider espionage, the motive alone is insufficient to explain this phenomenon. As Heuer (2001:n.p.) points out, there are many individuals in the intelligence community who would have a motive to engage in espionage, but there are few who actually do.

Secondly, rather than offering a systematically developed framework of factors that act as motives (or incentives as their counterparts), these approaches anecdotally focus on the motives and incentives that emerged in specific cases. This explains the overlap between the approaches as well as their differences. It also explains the reasons for the regular emergence of espionage motives and incentives that are not accounted for in any of these approaches (e.g. ingratiation in the case of Leandro Aragoncillo) (Defense Personnel Security Research Center, 2009:4). Thirdly, there also appears to be some confusion in terms of categorisation. Levchenko (1988:106) cites compromise and Smith (2017:5) cites adventurers, fantasists, and psychopaths as espionage motivational factors. While these variables may be connected to an individual’s motive to become a spy, they are, in and of themselves, not motives. Finally, these approaches only provide a static view in the sense that they state which motives may lead to acts of insider espionage or which positive incentives prevent it, but they do not provide insights into the process through which these motives are activated.

1.3.9 Personality approaches

Personality approaches may either exclusively focus on the personality characteristics of an insider spy, as in the case of the CIA’s ‘Project Slammer’ (Director of Central Intelligence, 1990:1-2); or personality in conjunction with other predictors - as in the approaches of Wilder (2017:20) and Houben (2003:278). Project Slammer was a 1990 CIA research programme aimed at better understanding of espionage by studying the personality characteristics of convicted spies (Director of Central Intelligence, 1990:1).

The full Project Slammer report remains classified, but a redacted initial report has been made public. According to the authors of the report, spies displayed several common characteristics. At the time of their involvement in espionage, the subjects believed that they are special and, in some cases, even unique. They had a sense of entitlement, believing that they were somewhat deserving. They felt that their situation was unsatisfactory, and that they had no other, or easier option than to engage in espionage. None of them regarded themselves as ‘a bad person’, and they believed that they were only doing what many others have done. They basically believed that their espionage activity was dissociated from their performance on the job. In their view, security procedures did not really apply to them, and security programmes were meaningless to them unless they could identify with such programmes (Director of Central Intelligence, 1990:2).

According to Wilder (2017:20), there are three factors associated with insider espionage: 1) personality dysfunctions, 2) a state of crises (i.e. a trigger), and 3) the opportunity to become a spy. Of these three factors, personality dysfunctions are at the core of Wilder's approach. According to Wilder (2017:20), an individual's personality factors (i.e., traits, attitudes, and values) are the key elements that determine whether or not an individual becomes a spy. The above author has also observed that personality dysfunctions and pathologies have frequently paved the way to espionage for individuals who have displayed excessive thrill-seeking, feelings of entitlement, or need for power and control.

Among some of its attributes, personality determines individuals' coping in moments of crises. Individuals with personality dysfunctions often choose paths to escape a desperate or painful situation, which manoeuvres them into even greater difficulty. Meanwhile, the opportunity factor includes both access to privileged information and a customer willing to provide what the individual needs in exchange for that information. To an individual with a dysfunctional personality and facing an acute crisis, engaging in espionage may appear to be the only, or easiest way to resolve the crises (Wilder, 2017:20).

Houben (2003:278) analysed the cases of 18 German women recruited by so-called 'Romeo spies' and were subsequently convicted on charges of espionage. It was Houben's (2003:278) objective to develop profiles of the targeted women on account of their personality profile and the incentives with which they were seduced. The personality variables in the above cases included 1) shyness, 2) religiousness, 3) intelligence, 4) political orientation, 5) adventurousness, 6) sexual disturbance, and 7) mental disturbance. On the other hand, the motives examined in the selfsame study were 1) love, 2) money and items of value, 3) compromise through misconduct, 4) sensitivity to subjectively perceived serious setbacks and lack of frustration tolerance, as well as 5) need for ego bolstering (Houben, 2003:276).

Approaches that focus on personality characteristics as a determining factor of insider espionage contribute a further important element in our understanding of the phenomenon of espionage. Clearly, personality characteristics can adversely influence self-control and reduce or negate an individual's inhibitions with respect to violating the law. Individuals with low sense of control may be prone to being insensitive, impulsive risk-taking, and inclined to short-sightedness, which may more likely render them to engage in criminality (Gottfredson & Hirschi, 1990:90).

An individual's personality is not the only factor that could have a disinhibiting effect. A strong emotional reaction to an event or situation can also affect behaviour (American Psychiatric Association, 2013:20; Deckers, 2016:41- 47 & 359; Keltner & Shiota, 2003:89). This is illustrated in the case of KGB Officer Oleg Gordievsky, who, by all accounts, appears to have had a stable personality and strong moral values. However, he offered to spy for the United Kingdom because he was infuriated *inter alia,* by the Soviet Union's invasion of Czechoslovakia in 1968 and was determined to contribute to the demise of what he considered to be a corrupt and oppressive system (Gordievsky, 2018:213).

Apart from personality characteristics, substance abuse and addictions can also lower the inhibition threshold and contribute to antisocial behaviour (American Psychiatric Association, 2013:20; Deckers, 2016:41-47, 359; Keltner & Shiota, 2003:89). This is illustrated in Aldrich Ames's case, a former CIA officer whose frequent lapses in judgement led to his illegal behaviour that was attributed to continuous and excessive alcohol consumption (Earley, 1997:136). Since inhibitions can be reduced not only by personality characteristics but also by other factors (e.g., alcohol abuse as in the case of Aldrich Ames), the researcher suggests that focussing exclusively on personality as a disinhibiting factor offers to narrow a view.

1.3.10 Situational approaches

Situational approaches place their primary focus on security measures that either facilitate or discourage insider espionage. Prunckun (2019:58-59) offers an example of a security situation consisting of a layered system of barriers (i.e., defence-in-depth), which aims to create inertia and cause spies to lose momentum as they encounter each barrier. This system consists of an outer layer of perimeter barriers (e.g. fences, lighting, razor-ribbons), an intermediate layer of access controls (e.g. speed styles and access cards), and an inner layer allowing information access exclusively on a need-to-know basis involving document classification and compartmentalisation (Prunckun, 2019:58-59).

According to Taylor (2007:8) counterintelligence theory at the governmental level is based on four assumptions:

1. Nations have decision-making systems based on information, which could jeopardise the nation's security if placed in the wrong hands;
2. The nation has one or more intelligence agencies that must prevent knowledge about their information from falling into the wrong hands;
3. Foreign intelligence agencies will try to obtain this knowledge; and
4. People must generally be regarded as possessing a very low level of trustworthiness (Taylor, 2007:8).

These assumptions have implications for the security systems that are put into place to protect a nation's interests. Taylor (2007:8) proposes a broader view than Prunckun's (2019:58-59) and suggests that a security system should include personnel security measures (pre-employment and in-service), facility security, communication security, classification, and compartmentalisation. Regarding communication security, however, some authors suggest using a broader perspective to include all relevant aspects of ICT. Similarly, Taylor's categories of classification and compartmentalisation could be regarded as very narrow, because they only address certain aspects that belong to the broader topic of information security. Rather than singling out these two aspects (classification and compartmentalisation), it is suggested that information security should be considered more broadly (Department of the Army, 2010:n.p.; Mehan, 2016:35-37; National Cybersecurity and Communications Integration Center, 2014:4; Olson, 2019:75; Secretary of the Air Force, 2019:11).

The approaches of Taylor (2007:5-6) and Prunckun (2019:58-59) address such situational vulnerabilities that might provide a spy with opportunities to steal information. In the researcher's view, these are valid considerations. However, these approaches do not consider factors such as motives, personality, market opportunities, or disinhibiting factors, which are addressed in other approaches and that are equally important for explanations pertaining to insider espionage (Director of Central Intelligence, 1990:1-2; Houben, 2003:278; Levchenko, 1988:106; Moore et al., 2016:1; Smith, 2017:5; Wilder, 2017:20).

1.3.11 Situation-disposition approaches

Situation-disposition approaches combine considerations related to the situation with those of the individual's disposition. The approaches of Pincher (1987:277-278), Herbig (2008:ix-xi) and Heuer (2001) can be associated with this category. Pincher (1987:277-278) asserts that insider espionage, which he refers to as treachery, is attributable to two factors: 1) access to privileged information and 2) motivation to commit the treachery. If an individual has access to privileged information and has the motivation to commit treachery, then the act of treachery will follow. Accordingly, Pincher (1987:277-278) expresses this relationship in logical notation as a material implication (→):

(1) $A + M \rightarrow T$,

where 'A' is access, 'M' is motivation and 'T' is treachery.

Pincher (1987:278) breaks down the complexity of motivation (M) into six distinct types: 1) money, 2) resentment, 3) 'blackmailability', 4) personality flaw, 5) self-satisfaction and 6) ideology; all of which extend the relationship to:

(2) $A + m + r + b + f + s + i \rightarrow T$,

where 'm' is money, 'r' is resentment, 'b' is 'blackmailability', 'f' is personality flaw, 's' is self- satisfaction and 'i' is ideology. In Pincher's view, it is the disposition that the individual has with respect to the motivational elements that will, in combination with the access to privileged information, determine whether the individual is vulnerable to becoming a spy.

Meanwhile, Herbig (2008) bases her approach on an in-depth study of 173 cases of espionage in the United States from 1947 to 2007 and identifies three relevant groups of variables that are predictors of insider espionage. Similar to the propositions by Levchenko (1988:106) and Smith (2017:5), Herbig (2008) includes a typology of motives in her approach. More closely aligned with the typology of Levchenko than that of Smith, Herbig's (2008:32) typology consists of seven motives, namely: 1) money, 2) divided loyalties, 3) disgruntlement, 4) ingratiation, 5) coercion, 6) thrill-seeking, and 7) recognition (ego).

Herbig's (2008:ix-xi) approach is distinguishable from that of Levchenko (1988:106) and Smith (2017:5) in that she adds two additional factors to her analysis. Apart from motive, Herbig (2008:32) also considers the possible vulnerabilities of an offender and the impact of important events that may act as triggers. Vulnerabilities are factors that can reduce an individual's natural inhibitions and render him or her more susceptible to acting unlawfully. Herbig's typology identifies six vulnerabilities: 1) lacking allegiance, 2) abuse of legal and illegal drugs, 3) alcohol abuse, 4) gambling addiction, 5) foreign influence/preference, and 6) financial issues (Herbig, 2008:40).

According to Herbig (2008:40), significant life events appear to have acted as triggers in about one third of the espionage cases she studied. These events typically occurred six to eight months before the offender became involved in espionage. In this category, Herbig (2008:40) includes negative events such as the 'death or terminal illness of a close friend or member of the family, separation or divorce from a spouse, lengthy physical separation from a spouse, marital discord … physical relocation, threatened suicide … a recent engagement or marriage, a new love relationship [and] an extramarital affair' (Herbig, 2008:42).

In contrast, Heuer (2001:n.p.) asserts that there are four factors related to insider espionage. The first is opportunity and its two-fold aspects. One aspect relates to the access that the individual has to privileged information. The other pertains to the offender's acquaintance with or easy access to individuals who have an interest in obtaining the information (Heuer, 2001:n.p.).

The second factor leading to insider espionage is that offenders must have a motive or a need that could be satisfied by engaging in the criminal activity (i.e., espionage). According to Heuer (2001:n.p.), this could be a financial need that could be fulfilled by selling the information to a foreign intelligence agency, or recognition in the event of an individual who has a need for heightened self-esteem (Heuer, 2001:n.p.). The third factor is that of the offender's ability to overcome natural inhibitions (Heuer, 2001:n.p.). Inhibitions can be reduced through a variety of conditions (e.g., feelings of entitlement, rationalisations, absence of the fear of being caught). The fourth factor in Heuer's approach is the trigger – an event that sets the offender's act of espionage into motion. Accordingly, insider espionage can only occur if all four conditions are met (Heuer, 2001:n.p.).

The approaches of Pincher (cf. 1987), Herbig (cf. 2008), and Heuer (2001:n.p.) are interesting because they broadly address important factors that facilitate insider espionage. Pincher (1987:277-278) includes access as a situational vulnerability and motivation with a variety of motives in his approach. In comparison with Heuer, Pincher does not, however, consider triggers, market opportunities (i.e. acquaintance with potential 'buyers'), or disinhibiting factors. Meanwhile, Herbig (2008:ix-xi, 32 & 40) considers triggers, motives, and personal vulnerabilities (i.e. disinhibiting factors), but not situational vulnerabilities or market opportunities. Additionally, Heuer (2001:n.p.) considers triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors, but does not provide a systematic view regarding any of these factors. Moreover, none of these approaches offer a systematic view to the range of motives or disinhibiting factors that may play a role in the characterisation of an insider spy. Furthermore, none of these approaches address the process through which an individual may become a spy.

1.3.12 Process approaches

In comparison with all of the previously discussed approaches, process approaches offer an interesting change in perspective because they appear less focussed on *'what'* causes an individual to become an insider spy, and more focused on *'how'* the individual becomes a spy. The approaches of Burkett (2013:11), Charney (2019:2-6) and Eoyang (1994:85-88) fall into this category.

In his approach, Eoyang (1994:85-88) describes a chain or process consisting of nine distinct behaviours that typically occur in espionage cases, provided that the spy is not apprehended before the process is completed. Accordingly, Eoyang 1994:85-86) posits these behaviours as: 1) development of the intention, 2) planning or conspiring to commit the crime, 3) gaining access, 4) acquisition of privileged information, 5) deception and concealing the spy's actions, 6) establishment of foreign contact, 7) exchange of information for some gain or expected gain, 8) consumption of the gain, and 9) escape in case of possible arrest.

Eoyang (1994:85-88) further asserts that the sequence of events could differ, depending on circumstances characterising the individual's involvement in the espionage activity. In the case of premeditated espionage, the sequence of events would follow the pattern listed above. However, should the offender become involved in espionage because he or she detects an unexpected opportunity, the steps involved in gaining access to privileged information (Step 3) and acquisition of that information (Step 4) would precede all other steps listed above. According to Eoyang, honeytrap operations would follow a different pattern as well. Gaining access (Step 3), establishing a foreign contact (Step 6) and consumption of a gain (Step 8) would precede the other steps which would follow in sequence (Eoyang, 1994:88).

Burkett (2013:11) acknowledges that the MICE approach provides some level of insight into the phenomenon of insider espionage but asserts that the approach does not capture the complexities of human motivation. This understanding can only be achieved if one focusses on the motivation process rather than the individual motivators. Burkett's (2013:11) approach draws heavily on the work of Cialdini (cf. 1984) who developed a concept aimed at explaining influence processes and persuasion. The novelty of Burkett's approach is the application of Cialdini's work to the recruitment of insider spies. Thus, Burkett (2013:11) regards the recruitment of spies as an influence process consisting of six steps: 1) reciprocity, 2) authority, 3) scarcity, 4) commitment, 5) liking, and 6) social proof (Burkett, 2013:11-17).

Charney (2019:2-6) describes the life cycle of an insider spy as a ten-stage process, the first six of which describe the stages leading to an individual's engagement in espionage activities: 1) sensitisation, 2) stress, 3) crises, 4) post-recruitment, 5) remorse, and 6) active espionage. Steps 7-10 relate to the discontinuation of the individual's spying activities (Charney, 2019:2-6). The author further suggests that spies often remain ensnared in espionage, with no exit option in sight, despite their effort to discontinue. Charney argues that operational security could be improved if individuals implicated in spy activities could find possible exit options for themselves, which would be most effective during Stages 2, 5 and 6 (Charney, 2019:2-6).

Process approaches offer an interesting perspective because they transcend the static concepts of other approaches by outlining the chain of events surrounding acts of insider espionage. These approaches, however, do not offer detailed systematic reflections on each variable or the dynamics within each individual stage. It is also not always evident how each factor might be operationalised. Nevertheless, they do help in providing an understanding concerning the fact that acts of espionage are not caused by a single factor (e.g. trigger, motive, situational vulnerability, market contact or disinhibiting factor), but by a variety of factors that are interconnected through some process (Burkett, 2013:11-17; Charney, 2019:2-6; Eoyang 1994:85-86).

1.3.13 Literature review summary

The foregoing literature review has brought several important points to light. Firstly, the approaches discussed here, collectively provide an important overview of the factors that can facilitate insider espionage. It is through this collectivity of factors that we come to realise that insider espionage cannot be adequately understood by focussing on one factor alone (e.g. motive or personality). Secondly, the approaches discussed here provide a valuable impression of the kind of variables that are instrumental in promoting insider espionage. However, the variables contained in each approach only appear to have been anecdotally collected, rather than systematically generated. Thirdly, some of the approaches suggest that insider espionage is the result of a process with milestones, but the relationships between the process on the one hand and the factors and variables on the other, largely remain unclear.

Based on the literature review, the researcher asserts that the variables jointly considered in existing theories of insider espionage revolve around five factors (themes): 1) triggers, 2) motives, 3) situational vulnerabilities, 4) market opportunities, and 5) disinhibiting factors. While it seems plausible that all five factors are necessary and possibly even jointly sufficient to explain insider espionage, the approaches vary substantially with respect to the factors that they consider. This is illustrated in Table 1.1 below, which shows the factors considered in each of the theories, as well as the existing gaps in current literature. Of the fourteen theories listed in the table, only Heuer's (2001:n.p.) considers variables that are associated with each of the five factors. The second observation is that Heuer's (2001:n.p.) approach also offers only examples of relevant variables, which is far from offering a comprehensive overview of the relevant variables associated with each of the factors. Moreover, the treatment of the variables that influence someone to become an insider spy are often unsystematic, inaccurately categorised, and frequently explained insufficiently.

This concern is particularly relevant with respect to approaches covering motivation, disinhibiting factors, and situational vulnerabilities. Finally, only three of the fourteen approaches discussed in Section 1.3.12. (i.e. Burkett, 2013:11-17; Charney, 2019:2-6; Eoyang, 1994:85-86) address the process by which an individual may become involved in insider espionage. While their focus on process is a valuable contribution to our understanding, these approaches are also not comprehensive since none of them consistently reflects the full range of factors.

Table 1.1: Factors considered in insider espionage models

Aspects **Authors**	**Factors**					**Process**
	Triggers	Motives	Situational Vulnerabilities	Market Opportunity	Disinhibiting Factors	
Levchenko (1988:106)		X				
Smith (2017:5)		X				
Moore et al. (2016:1)	X	X	X			
DCI (1990:1-2)					X	
Wilder (2017:20)	X		X	X	X	
Houben (2003:278)		X			X	
Prunckin (2019:58-59)			X			
Taylor (2007:5-6)			X			
Pincher (1987)		X	X			
Herbig (2008:ix-xi, 32 & 40)	X	X			X	
Heuer (2001)	X	X	X	X	X	
Eoyang (1994:85-86)			X	X	X	X
Burkett		X				X

(2013:11-17)						
Charney (2019:2-6)	X					X

(Source: Compiled by the researcher)

In the researcher's view, it is only through the consolidation of these factors into a single conceptual framework, that insider espionage can truly be understood and acts of insider espionage can be predicted. Such a framework entails the systematic grasp of the constituent variables, free of gaps, overlaps and misalignments, as well as the unambiguous definition and in-depth understanding of the factors and their attendant variables.

1.4 PURPOSE OF THE RESEARCH

A research purpose statement should provide the reader with insight concerning the researcher's reasons or justification for undertaking a given study, as well as the intended accomplishment through the particular study (Creswell, 2014:123). To the reader, the purpose statement should provide an unambiguous indication of the target that the researcher intends to reach. In doing so, the research purpose statement should also help in directing the expectations of the reader (Denscombe, 2019:39). For Wilson (2014:43), the research purpose is the broad statement by the researcher concerning some definitive information on some aspect/s pertinent to the investigated subject matter or phenomenon. In this regard, the present study fulfils the purpose of exploration and description/explanation; forecasting an outcome; and evaluation of a current situation, amongst other purposes. These three critical purposes are interstitial to the research topic in its entirety.

1.4.1 Exploration and description/explanation

This aspect of the research purpose occurs in view of the deficiencies in the current body of literature outlined in Sub-section 1.3.13. In its ontological sense then, exploration entails the researcher's protracted search for more information and details concerning the fundamental characteristics of the core research variables in the investigated phenomenon, such as espionage in its multifactorial contexts (i.e., manifestation and implications) (Wilson, 2014:43). It is in this specific regard that the present research seeks to explore the independent variables (predictors) that must be present for insider espionage to occur.

Additionally, the aspects of description and explanation (used interchangeably and synonymously here) entail the researcher's provision of answers or details concerning aspects of the phenomenon being investigated (i.e., insider espionage) (Durrheim & Painter, 2016:47). Therefore, both the explanatory and descriptive aspects of research are complementary to the explorative aspect, with the latter (exploration) preceding the former (explanation and description) aspects. To that effect, the current study fulfils the purpose of explaining and describing the relationships between the independent variables (predictors) and insider espionage, which is regarded as the dependent variable in this study.

On the whole, therefore, both the exploration and description/explanation of the independent variables (predictors), serve as the catalytic factors for understanding the *what, where, who, why*, and *how* of the theoretical and practical factors that ought to materialise for insider espionage to occur; all of which constitute a substantial part of Chapter 3's focus.

1.4.2 Forecasting an outcome

Forecasting an outcome is associated principally on the study's focus on predicting possible future consequences emanating from particular patterns of behaviour and other variables (Efron & Ravid, 2019:37). This aspect of the research purpose is manifested in the construction of an interdisciplinary conceptual framework that represents the independent variables (predictors) and their relationships in order to predict risks of insider espionage. To that effect, Chapter 4 is the principal domain in terms of which the forecasting of an outcome is situated as one of the study's main research purposes.

1.4.3 Evaluation of a current/existing situation

Evaluating a current or existing situation entails that different situations are compared and contrasted for the purpose of enabling an objective framework of conclusions and findings (Denscombe, 2019:39). As such, the interdisciplinary conceptual framework referred to in the preceding Section 1.4.2 is validated by applying it to a selection of specific cases of insider espionage to identify the degree of presence of the insider espionage predictors as detailed in Chapter 5.

1.5 RESEARCH QUESTIONS

In Section 1.2.1, insider espionage was contextualised and shown to be a considerable threat with potentially dramatic consequences. The literature review in Section 1.3 discussed existing theories explaining insider espionage and suggested that they are fraught with a variety of deficiencies. These theories do not satisfactorily explain *how* insider espionage occurs, or *how* risks of insider espionage can be predicted. The deficiencies in existing literature, led to the research purpose outlined in Section 1.4. Accordingly, the present research aims to answer the ensuing four below-cited questions that accrue from the stated research purpose:

> **Question 1**: What are the independent variables that are predictors of insider espionage (dependent variable) in the government and private sectors?
> **Question 2**: What are the relationships between the variables of insider espionage in the government and private sectors?
> **Question 3**: How can the variables of insider espionage and their relationships be represented in an interdisciplinary conceptual framework that can serve to predict risks of insider espionage?
> **Question 4**: How can the interdisciplinary conceptual framework be applied to specific cases of insider espionage to identify the presence of predictors of insider espionage, and thereby validate the conceptual framework?

1.6 RESEARCH OBJECTIVES

The purpose of stating the research objectives is to highlight the specific phenomenon being investigated and its linked variables that will be the focus of the research (Creswell & Creswell, 2018:206). Objectives should convey how the learning will take place (e.g. explore, examine, discover) and the goals that each of the objectives should ultimately reach (Creswell & Creswell, 2018:206 & 240). Based on the foregoing, this research aims to achieve four objectives:

- Objective 1: to explore the independent variables that are predictors of insider espionage (dependent variable) in the government and private sectors.
- Objective 2: to explore the relationships between the variables of insider espionage in the government and private sectors.
- Objective 3: to construct an interdisciplinary conceptual framework that represents the variables of insider espionage and their relationships, which can serve to predict risks of insider espionage.

- Objective 4: to explore the application of the interdisciplinary conceptual framework to specific cases of insider espionage in order to identify the presence of predictors and thereby validate the conceptual framework.

1.7 DELIMITATIONS OF THE STUDY

Denscombe (2019:57-58) highlights the importance of delimiting and restricting the scope of the research to be performed. Readers ought to be informed what will, and will not be included in the research, and reasons for such inclusion boundaries. In this study, there are five delimitation aspects that warrant consideration: 1) the organisational boundaries, 2) the boundaries related to the subjects, 3) the geographical boundaries, 4) the temporal boundaries, and 5) boundaries related to literature. These are discussed in the following subsections.

1.7.1 Organisational delimitations

Pfeiffer (1997:9) defines organisations as social entities that 'have a goal of survival and self-perpetuation … clearly defined, demarcated, and defended boundaries, and often (although not invariably) have some formal relationship with the state that recognises their existence'. In principle, any kind of organisation could be the target of insider espionage. Most frequently, however, espionage is targeted against 1) governmental (including military) organisations, 2) commercial/industrial organisations, 3) academic/research organisations, and 4) multilateral international organisations such as the United Nations, African Union, or European Union. It is through espionage against these types of organisations that the greatest amount of damage is incurred (Bundesamt für Verfassungsschutz, 2017:n.p.; Director of National Intelligence, 2019:n.p.; Gowan, 2018:n.p.). In light of the frequency with which they are targeted, and the resultant damage caused, the focus of this research is on the four types of organisations cited above. Other types of organisation, like political parties, interest groups, and professional associations are not included in this study.

1.7.2 Delimitation related to subjects

There are two subject-related points to be addressed: 1) the type of spies that will be studied, and 2) the population that will be studied within that category. Firstly, the scope of this research is limited to the population of insider spies. These are members (employees or officers) of organisations who could gain access to their organisations' privileged information and who, after joining the organisation, have volunteered or have been recruited to provide such information to an unauthorised third party. This includes spies in the classical sense as well as whistle-blowers. However, bearing in mind that whistle-blowers fulfil an important function worthy of protection, this study only includes such whistle-blowers who – without due cause - by-pass their organisation's whistle-blower guidelines. Other types of spies are not part of this study because the relevant factors are likely to be substantially different. This relates to operatives who have been dispatched with the specific objective of infiltrating a target organisation, or individuals who act as informants or assets for governmental organisations within their own countries. The second point is concerned with access to data on the research population. Not all insider spies are caught. If caught, it does not necessarily follow that their cases will be made public. Within the realm of this study, the researcher only considered the publicly known cases for which an adequate amount of reliable information is available in the public domain.

1.7.3 Geographical delimitation

The purpose of this research is *inter alia* to validate an interdisciplinary conceptual framework of insider espionage by applying it to a selection of specific cases and through this to identify the presence of predictors. Towards this end, the researcher initially cast a wide net to capture as many case histories as possible. Using a variety of sources, the researcher was able to find references to 258 cases of insider espionage in 12 countries. However, 40 of these cases were finally discarded because they did not fall within the previously outlined delimitations. While this did reduce the number of cases to be considered to a total of 218, it did not affect the number of countries, which remained the same.

1.7.4 Temporal delimitation

The discussion of globalisation in Section 1.3.3 and the developments in the field of ICT in Section 1.3.6 have shown how the world has changed after the Cold War It is important to realise that these developments have also had an impact on insider espionage. In light of these developments and the impact that they have on the zeitgeist and the *modus operandi* of insider espionage, the emphasis of this study is on cases that have come to light after the end of the Cold War. However, since there are discernible trends with respect to the use of ICT and the impacts of globalisation on insider espionage, it is the researcher’s view that these can be brought out more clearly by referencing Cold War insider espionage cases as a form of baseline. For this reason, Cold War cases will also be considered where it appears relevant for the discussion.

1.7.5 Literature-focused delimitations

There are three points that should be addressed with respect to the literature used in this study. The first is related to the amount of literature available on the proposed subject matter. As pointed out by Johnson (2014:9-10), intelligence is a comparatively novel field of inquiry. The amount of literature available appears very limited, especially when compared to the abundance of literature available in other disciplines. The literature review provided an indication of what is presently available in theories or conceptual frameworks of insider espionage. While the amount of theoretical material pertaining to insider espionage is clearly limited, there is an abundance of material describing the circumstances surrounding specific cases of insider espionage. This has proven to be a rich source of data. Furthermore, there is the type of literature that has been used in this study to analyse specific cases of insider espionage; that is, case-specific documentation that is also available in the public domain.

In this study, classified or otherwise restricted documents have not been analysed. With these caveats, the case-related documents used in this study fall into three categories: 1) court and other official documents, 2) historical accounts, biographies, and autobiographies, and 3) news reports from a wide range of news providers. The volume, scope, and credibility of documents related to the selected cases have been carefully examined. Cases lacking with respect to these considerations were dismissed. The third point relates to the languages in which the evaluated documents have been written. The researcher is fluent in English and German. The literature reviewed by the researcher has, therefore, primarily been in these two languages.

1.8 DEFINITION OF KEY TERMS

Defining the key terms applied in the research helps the reader understand the researcher’s contextual, lexical, discipline-specific, and practice-related usage of the terms considered important to the research topic. Such terms are typically defined in a dedicated section of the research and should be the object of precise language based on authoritative sources (Creswell & Creswell, 2018:40-41). The following constitute key terms that are used in this research.

1.8.1 Economic espionage

Economic espionage is a criminal act in which an individual ‘‘… intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly— 1) steals, or without authorisation appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; 2) without authorisation copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; 3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorisation; 4) attempts to commit any offense described in any of paragraphs 1) through 3); or 5) conspires with one or more other persons to commit any offense described in any of paragraphs 1) through 3)…“ (United States Congress, 1996:3488-3489).

1.8.2 Espionage

Espionage is the clandestine collection of information (Bennett, 2003:96). It is an act deemed to have been committed by a person if: ‘(a) the person deals with information or an article; and (b) the information or article: (i) has a security classification; or (ii) concerns … national security; and (c) the person intends that the person’s conduct will: (i) prejudice … national security; or (ii) advantage the national security of a foreign country; and (d) the conduct results or will result in the information or article being communicated or made available to a foreign principal or a person acting on behalf of a foreign principal’ (Parliament of Australia, 2018:26).

1.8.3 Foreign intelligence agency

A foreign intelligence agency is ‘an intelligence or security service (however described) of a foreign country’ (Parliament of Australia, 2018:47).

1.8.4 Foreign principal

A foreign principal is ‘(a) a foreign government principal; (aa) a foreign political organisation; (b) a public international organisation…; (c) a terrorist organisation…; (d) an entity or organisation owned, directed or controlled by a foreign principal within the meaning of paragraph (aa), (b) or (c); (e) an entity or organisation owned, directed or controlled by 2 or more foreign principals within the meaning of paragraph (a), (aa), (b) or (c) (Parliament of Australia, 2018:23).

1.8.5 Handler

A handler is a ‘case officer who is directly responsible for the operational activities of agents’ (Bennett, 2003:125). The terms handler and controller are often used interchangeably (Bennett, 2003:60).

1.8.6 Intelligence agency

An intelligence agency is an ‘… organisation, or its subordinate parts, primarily responsible for or engaged in the collection of information; the processing of that information into intelligence and the subsequent dissemination of the intelligence produced’ (Director of Central Intelligence, 2003:5).

1.8.7 Intergovernmental organisation

An intergovernmental organisation (IGO) is an ‘entity created by treaty, involving two or more nations, to work in good faith, on issues of common interest’ (Harvard Law School, 2019).

1.8.8 Insider espionage

Insider espionage is perpetrated by an employee with legitimate access to his or her organisation’s privileged information and who steals such information for personal gain (Federal Bureau of Investigation, n.d.:1). Insider espionage is any type of espionage in the meaning of 1.8.1 or 1.8.2 above.

1.8.9 Insider spy

An insider spy is an individual who commits insider espionage in the meaning ascribed to Section 1.8.8 above.

1.8.10 Intelligence officer

An intelligence officer is a civil servant who is an official member of, and employed by an intelligence service (Smith, 2017:306).

1.8.11 Predictor

A variable ‘used to estimate, forecast, or project future events or circumstances. This term sometimes is used interchangeably with independent variable’ (APA, 2020).

1.8.12 Risk

A risk is a ‘measure of the potential degree to which protected information is subject to loss through adversary exploitation’ (Secretary of the Air Force, 2020:58).

1.9 CHAPTER LAYOUT

The thesis is structured according to the following six chapters:

Chapter 1: General introduction to insider espionage in the government and private sector

The aim of this chapter is to introduce the subject of insider espionage and its associated issues, namely: the research problem; preliminary review of literature; the research purpose, questions, objectives, and delimitations; as well as the definition of key terms. These elements lay a foundation for the ensuing chapters.

Chapter 2: Methodological framework of the study

The chapter principally focuses on the methodological framework adopted by the researcher in conducting his study. In this regard, the researcher addresses four philosophical worldviews; the research design; sampling; data collection, analysis, and interpretation; as well as the trustworthiness and ethical issues of the study.

Chapter 3: Exploring the variables of insider espionage and the relationships between them

The chapter essentially analyses the insider espionage variables and the associated relationships between these variables.

Chapter 4: Development of a conceptual framework of insider espionage

This chapter encompasses the researcher's developed conceptual framework to analyse and predict insider espionage.

Chapter 5: Case study analysis

In this chapter, the researcher applies his developed conceptual framework to four actual cases of insider espionage and thereby aims to validate the conceptual framework.

Chapter 6: Findings, recommendations, and conclusion

In this final chapter of the study, the researcher reports on his main findings, proposed recommendations accruing from the findings, and the conclusion of the study.

CHAPTER 2: METHODOLOGICAL FRAMEWORK OF THE STUDY

2.1 INTRODUCTION

The current chapter outlines the methodological framework that is used in this study. This discussion articulates the philosophical worldview espoused by the researcher and elaborates the research design that is being used to actualise the purpose of this study and to address the research questions and objectives.

2.2 PHILOSOPHICAL WORLDVIEW OFFERED IN THE STUDY

Creswell and Creswell (2018:5) assert that research should contain the larger philosophical ideas that the researcher espouses. Guba (1990:17) defines a worldview as a 'basic set of beliefs that guide action'. By espousing their worldviews, researchers lay the foundation and provide the reasoning for their choice of research approach. Some authors regard the terms, 'paradigm' and 'worldview' as synonymous (Creswell & Creswell, 2018:5).

Slife and Williams (1995:1) suggest that behavioural sciences study and seek to explain a broad range of human behaviours. With respect to any social behaviour, however, these authors observe that different researchers espouse different explanations of the behaviour they are studying, which is attributable to variations in the way each researcher views the world. In the understanding of Guba and Lincoln (1994:107), a worldview defines how a researcher perceives the world, the individual, and the relationships between the individual and that world, or parts of it. In this sense, Leavy (2017:11) regards a worldview as a set of foundational perspectives which carry a set of assumptions and guide the research process. Despite the criticality of the researcher's worldview in the formulation and use of theories, such views are often left implicit in the work presented by researchers (Slife & Williams, 1995:1-2).

2.2.1 Four worldviews

According to Creswell and Creswell (2018:6), worldviews largely fall into four mainstream categories: 1) post-positivist worldview, 2) constructivist worldview, 3) transformative worldview, and 4) pragmatist worldview. Crotty (1998:10) emphasises that worldviews contain a researcher's epistemological beliefs, which should be made explicit. The above-cited author asserts further that an epistemological standpoint coexists with, or is influenced by the researcher’s ontological beliefs. For Leavy (2017:10), both the ontological and epistemological beliefs of the researcher also ought to be explicit. The following section discusses the main worldviews proposed by Creswell and Creswell (2018:6), and also outlines the associated ontological and epistemological beliefs.

2.2.1.1 Post-positivist worldview

The post-positivist worldview represents a traditional approach to research. This worldview challenged the traditional worldview of positivism in that it disputes the notion of the absolute truth of knowledge. Proponents of the post-positivist worldview have argued that it is not possible for science to be positive about any claims of knowledge with respect to the behaviour of human beings (Creswell & Creswell, 2018:37).

Post-positivists maintain that reality can only be understood probabilistically. This ontological view is complemented by an epistemology that asserts the notion of a separation of the investigator and the object of investigation should be abandoned - as claimed by the positivists - but that objectivity should still be pursued (Howell, 2013:29).

2.2.1.2 Social constructivism

Social constructivism is a paradigm which is associated with a *relativist ontology*. According to this worldview, there is not just one, but a multitude of realities. They exist as a multitude of intangible mental constructions that are based on social interactions and the experiences of the individual. Reality is thus dependent on the person or group of persons who hold these mental constructions that are merely ‘more or less informed and/or sophisticated’ (Guba & Lincoln, 1994:111-112).

Epistemologically, social constructivism is *transactional* and *subjectivist*. This means that there is no separation between the investigator and the subject. They interact with each other. Findings generated through the research of the investigator emerge during the investigation (Guba & Lincoln, 1994:111-112).

2.2.1.3 Transformative worldview

The transformative worldview is a position that was advanced during the 1980s and 1990s. Proponents of this worldview hold that post-positivist assumptions emphasise methods that cannot adequately address individuals or groups who are marginalised in society, or issues of the distribution of power and social justice, discrimination, and oppression. The transformative worldview often focuses the work of researchers on demographic issues facing individuals or groups in respect of their gender, ethnicity, race, socioeconomic status, disability, and sexual orientation; all of which engender skewed power relationships. Advocates of this worldview assert that the constructivist position does not adequately support action agendas that would benefit marginalized groups (Creswell & Creswell, 2018:9).

Reflecting on the philosophical elements of critical theory may offer a useful starting point to address the diverse issues faced by marginalised groups. According to Creswell and Creswell (2018:62), critical theory is largely focused on empowering individuals and groups to overcome their demographically imposed constraints. Ontologically, this theory is associated with a perception of reality that is shaped by history and formed by values that emerged over time (i.e., historical realism). The epistemological view of this theory suggests that the investigator and the subject are linked, and that historical values influence the investigator's inquiry, resultantly producing subjective results (Howell, 2013:29; Killan 2013:22).

2.2.1.4 Pragmatist worldview

The pragmatism worldview is premised on situations, actions, and consequences, and not antecedental conditions as in the post-positivist sense. Pragmatism is focused on practical applications and problem-solving. In that regard, this paradigm does not advance any specific system of philosophy and reality (Creswell & Creswell, 2018:10- 11). Furthermore, pragmatists believe 'there is an external world independent of our minds', as well as a reality that is lodged in the mind (Cherryholmes, 1992:14). Proponents of this worldview emphasise the 'importance [of] focusing attention on the research problem in social science research and then using pluralistic approaches to derive knowledge about the problem' (Creswell & Creswell, 2018:10-11). In a methodological context, researchers espousing pragmatism are 'free to choose the methods, techniques, and procedures of research that best meet their needs and purposes… [They] look to many approaches for collecting and analysing data rather than subscribing to only one way [e.g., quantitative or qualitative]' (Creswell & Creswell, 2018:10-11).

2.2.2 Applying the pragmatic worldview to this study

The researcher subscribes to a pragmatic worldview because it is consistent with his view of the world and also allows incorporation of results established through other worldviews and methodologies. In the researcher's view, this is essential to build the body of knowledge necessary for fully understanding the phenomenon of insider espionage.

The approach applied by the researcher is qualitative and emphasises a hermeneutic methodology, which could suggest a constructivist worldview. However, while performing the research, the researcher has not only drawn on the results of other researchers who have performed their inquiry within the framework of a qualitative study; but also drawn on the results of quantitative research related to insider espionage. If the researcher was to oppose a positivist or post-positivist worldview, he would also have to dismiss any quantitative research to remain consistent (e.g., Herbig, 2008; Houben, 2003) that is based on this worldview. In the researcher's view, the findings of such studies are too valuable for the comprehensive understanding of insider espionage to be dismissed only because they do not conform to a specific worldview.

2.3 RESEARCH DESIGN

Lincoln and Guba (2013:37) assert that researchers concerned with the nature of knowledge and inquiry must not only address their ontological and epistemological viewpoint, but also their methodological approach. Thus, the question they must answer is how they intend to acquire their knowledge. According to Howell (2013:24-30) and Killam (2013:109), the term, 'methodology' denotes an approach to systematic inquiry which is driven by the researcher's worldview. For this reason, both Howell (2013:24-30) and Killam (2013:109) assert that methodologies can be aligned with worldviews. This assertion is supported by Guba and Lincoln (1994:24). Table 2.1 outlines the methodologies that correspond with post-positivism, constructivism, and critical theory.

Table 2.1: Worldviews and methodologies

Worldview	Methodology
Post-positivism	Modified approach to scientific experimentation, pursuing the falsification of hypotheses.
Constructivism	Qualitative: hermeneutical methodology; creating consensus through individual constructions.
Critical Theory	Dialog-based and dialectical methodology.

(Sources: Guba & Lincoln, 2004:24; Howell, 2013:29; Killam, 2013:109)

Creswell and Creswell (2018:10) suggest that pragmatism is not associated with any one ontology or epistemology. In this regard, the researcher is at liberty to draw from both quantitative and qualitative assumptions and employ the corresponding methodologies accordingly. The researcher subscribes to a pragmatic worldview and has argued in the previous section that this worldview opens the option of considering data from methodologies, which in his opinion would otherwise have to be dismissed.

2.3.1 Research approach

Research approaches are broadly categorised into three groups: 1) qualitative research, 2) quantitative research, and 3) mixed-methods research. Qualitative research enables the exploration and understanding of social and human problems (Creswell, 2014:4). It aims at searching for, reconstructing, and interpreting the subjective meaning of individual experiences (Killam, 2013:226). In contrast, quantitative research is used for testing theories through the examination of relationships between variables of the theory (Creswell, 2014:4). This approach centres on objectivity, control, and precise measurement (Leavy, 2017:87). Mixed method research advances both quantitative and qualitative research methods by collecting and integrating data through both (Leavy, 2017:164).

As outlined in Section 1.4., the purpose of this research is to: 1) explore the independent variables (predictors) that must be present for insider espionage (dependent variable) to occur, 2) explain the relationships between these variables, 3) construct an interdisciplinary conceptual framework that represents these variables and the relationships between them and that can serve to predict risks of insider espionage, and 4) validate this interdisciplinary conceptual framework by applying it to a selection of specific cases of insider espionage to identify the presence of predictors of insider espionage. To fulfil the first two of these objectives, the researcher has chosen to draw on prior research, which in some cases was based on qualitative and in others on quantitative research. In the researcher's understanding, this is commensurate with the pragmatist worldview outlined in Section 2.2.2.

Deciding on a research approach narrows the field of possible research designs. The present study is qualitative and aims to help exploration and understanding of social and human problems (Creswell, 2014:4). The researcher then considers it appropriate to adopt and utilise a qualitative research design to advance this study's overall intentions. Creswell and Creswell (2018:12) suggest that there are five designs associated with qualitative research:

- Narrative research, which is a form of inquiry used in the humanities to study the lives of individuals and to capture their stories in a narrative.
- Phenomenological research, which is cognate from the fields of philosophy and psychology. Researchers in this field collect data about the lived experiences of individuals with respect to a specific phenomenon. The descriptions are based on the subject's narrated accounts and serve to capture the essence of experiences.
- Grounded theory, which is cognate from sociology and is a form of inquiry in which research generates abstract theories that are grounded in the view of participants that are typically related to processes, actions, or interactions.
- Ethnography, which is a form of inquiry that originates in anthropology and sociology. In this type of inquiry, the focus is on intact cultural groups in a natural setting and aims to study common behavioural patterns, language, and actions over a prolonged period.
- Case study, which is a form of inquiry found in many fields. In case study research, the focus is on developing an in-depth analysis of events, activities, or processes, which may involve one or more individuals. The cases are bounded with respect to the time frame and the event, activity, or process. The researcher collects detailed information on his or her case using various data collection procedures over an extended period (Creswell & Creswell, 2018:12).

The researcher chose the case study design because it offers the greatest opportunity for in-depth analysis of events, activities, or processes that involve one or more individuals. However, the analysis of a single case would not have been sufficient to achieve data saturation. The researcher, therefore, adopted a multiple-case study approach which he concluded with a cross-case analysis.

In the present research, the case analysis would have been conducted on the basis of an existing theoretical framework which addresses all constructs relevant to the prediction of insider espionage and the relationships between these constructs. However, following the literature review of existing theories of insider espionage, the researcher concluded that no such framework exists. It was for this reason that the researcher built a conceptual framework and developed a theory of insider espionage that could be used to study the cases.

According to Jaccard and Jacoby (2010:39,75 & 91), theory construction and model building consists of three processes which were also applied in this study. The first process involves developing ideas regarding new explanatory constructs and their relationships (Jaccard & Jacoby, 2010:39). This was achieved through the literature review of current theories of insider espionage, and combining the variables that each of the theories contain into a comprehensive preliminary framework. The second process involves focussing concepts by ‘specifying and refining conceptual definitions for those concepts that one decides to include in the theoretical system’ (Jaccard & Jacoby, 2010:75) and the third process involves clarifying the relationships between the concepts (Jaccard & Jacoby, 2010:91). These processes were completed through a thorough review of relevant interdisciplinary literature in the fields of psychology, psychiatry, political science, law, economics, and security studies.

2.3.2 Research population

The term population denotes a ‘group of elements about which the researcher might later make claims’ (Leavy, 2017:255). The population in this study consists of individuals who have been engaged in insider espionage. The sampling population (sampling frame), which is a subset of the population, is the ‘group of elements from which the sample is actually drawn’ (Leavy, 2017:255). In this study, the sampling frame includes cases of insider espionage that have become known to the public, and that have been documented in publications (biographical and autobiographical materials, court documents, official commission reports, and video-recorded interviews that are available online) in the English or German languages regardless of the country in which the espionage occurred.

2.3.3 Sampling

Leavy (2017:255) defines sampling as the process in which ‘a number of individual cases are selected from a larger population’. Sampling addresses who or what will be considered in the study and the sources from which the researcher will be getting his or her data (Leavy, 2017:75). Accordingly, the samples in this research have been drawn from publicly available literature on cases of insider espionage.

The researcher opted for the use of theoretical sampling in this study. This sampling approach follows an iterative procedure of data gathering, analysis and further data gathering until the category under investigation reaches the point of saturation. Saturation is considered to have been reached when no new categories or relevant themes emerge from further data analyses and the categories show depth and variation (Corbin & Strauss, 2008:148-149). Theoretical sampling is particularly suitable for exploratory studies when a researcher wishes to study new and largely uncharted areas because it allows for further discovery of pertinent details about the investigated phenomenon.

Most importantly, theoretical sampling allows for researchers to take advantage of fortuitous events – instances in which relations between variables are discovered that may have remained hidden if more conventional methods of sampling had been used (Corbin & Strauss, 2008:145-146). Throughout the theoretical sampling process, the researcher should choose data that bears ‘the greatest potential to capture the kinds of information desired’ (Corbin & Strauss, 2008:151). The choice of sample results from the researcher’s pursuit of an analytical trail in which the researcher travels from lead to lead (Corbin & Strauss, 2008:146).

In this study, the researcher drew on the list of espionage cases contained in Annexure A. Initially, the researcher randomly selected cases from this list and in the sequence of selection, reviewed the volume of literature that is available in the public domain with respect to each case. Through this process, the researcher identified three cases for which a sufficient amount of literature was available. These were the cases of Aldrich Ames, Oleg Gordievsky, and Werner Stiller. After an initial analysis of each of the cases, it became evident that all three cases had begun during the Cold War and ended during, or shortly thereafter.

Aspects related to globalisation and developments in the field of ICT, which are key features of espionage in today's society, were largely absent. Moreover, the third case selected by the researcher, that of Werner Stiller, brought no significant additional data to light. In ensuring the relevance of the study with respect to the current situation, the researcher discarded the analysis of the Stiller case and restarted the random sampling process by specifically searching for espionage cases that have occurred in the 21st century, and that were most likely to contain strong globalisation and ICT elements. Again, the researcher screened the case material in sequence and retained the two cases, those of Brian Regan and Edward Snowden, that held the greatest promise in terms of the volume of case material that was available in the public domain.

2.3.4 Data recording

The researcher used the MaxQDA software programme to record the data. MaxQDA is a programme which allows the researcher to record texts, pdf documents, tables, images, and media. It can also be used to import transcripts, surveys, and websites. This product proved to be a good choice because it allows the initial recording of the data (which is important during data collection), and also supports data analysis (discussed below). In addition, the MaxQDA programme also offers a considerable amount of support, including a comprehensive user manual, online tutorials, and online user support (MaxQDA, 2019:n.p.).

2.3.5 Data collection

Creswell and Creswell (2018:188-189) distinguish between four sources of qualitative data collection: 1) observation, 2) interviews, 3) documentation, and 4) audio-visual material. Due to the clandestine nature of espionage, observations clearly did not present a viable option. Interviewing intelligence officers, investigators or individuals convicted of espionage was also not viable. The identities of intelligence officers and investigators are typically protected. Moreover, the knowledge that they would have of specific cases would most likely be classified, therefore, not be accessible to be published by the researcher.

Efforts to identify the names and whereabouts of individuals convicted of insider espionage in Germany (the researcher's place of residence) have remained without success because of German privacy laws that limit the publication of the last name of convicted felons without their consent. The study was, therefore, conducted with data contained in documents and audio-visual materials. This is consistent with most other work performed in the field of intelligence, which relies heavily on documents available to the public, similar to research in the field of history (Warner, 2007:22). In this regard, the researcher relied mostly on biographical and autobiographical materials, court documents, official commission reports, and video-recorded interviews that are available online in analysing the case studies.

2.3.6 Data analysis

Data analysis involves the detailed examination of data that has been extracted from data sources (Strauss & Corbin, 1998:58). It is the process according to which researchers make sense of the data that they have collected by dissembling it and assembling it back (Creswell & Creswell, 2018:190-192). For the purpose of this study, the researcher adhered to the following data analysis process:

- Simultaneous procedures consisting of data collection, analysis, and write-up of the findings during which each document or media item was examined, coded and key findings were recorded or documented in a memo at the time of collection (Creswell & Creswell, 2018:192);
- Data winnowing processes for separating relevant from irrelevant data and then disregarding the latter. As proposed by Creswell and Creswell (2018:192), the researcher found that winnowing was necessary because texts were so rich with information, but only parts of these texts were useful for the qualitative study; and
- Hermeneutics as a process aimed at understanding the meaning and significance of a subject's experiences, dispositions, and motives, which in turn gave rise to a subject's projects and goals (Glynn, 2017:315-316).

The data analysis procedure implemented by the researcher consisted of five steps: 1) organisation and preparation of the data for analysis, 2) data review, 3) data coding, 4) generation of descriptions and themes, and 5) representation of the descriptions. Organisation and preparation of case specific data followed the selection of the case from a list of espionage cases (see Annexure A). This included visually scanning documents that related to the case under consideration and preparing them for the subsequent data review (Creswell & Creswell, 2018:193).

Data review involved gaining a general sense of the information provided by the data. The researcher read and evaluated all available material related to the selected case. This step served to capture the content, and forming impressions of the overall density of the information available and to assess its credibility (Creswell & Creswell, 2018:193). This was an important step because the volume, scope, and credibility of the data available to the researcher was varied. Coding involved the organisation and bracketing of voluminous textual information, and writing a word or code representing a category (Creswell & Creswell, 2018:193).

The codes and definitions used by the researcher are listed in Annexure B. The next step involved the detailing of relevant information on the various cases examined in this study, and developing transversal themes and subthemes from findings based on the codes (Creswell & Creswell, 2018:194). This theme-based approach can be seen in Chapter 5, in which the cases of Oleg Gordievsky, Aldrich Ames, Brian Regan, and Edward Snowden were analysed in detail. In the final step, the descriptions and themes were represented in the form of a cross-case analysis. Emphasis was placed on the interconnections between the categories, which was used to build a conceptual framework of insider espionage. This was achieved by applying an approach advanced by Eisenhardt (cf. 1989) which involves searching for cross-case patterns, performing and iterative tabulation for each construct as well as the search of the reason for relationships.

2.3.7 Data Interpretation

In this study, interpretation is two-fold. The one interpretation is focused on the processes involved in the development of the conceptual framework and theory used to explore cases of insider espionage (see Jaccard & Jacoby, 2010:39,75 & 91). The second interpretation premised on the interpretation of data that was extracted from specific cases of insider espionage.

Based on data interpretation procedures suggested by Creswell and Creswell (2018:198-199), Chapter 6 provides a summary of the findings, recommendations, solutions, and a conclusion of the study.

2.3.8 Trustworthiness of the study

Lincoln and Guba (1985:300) posit that trustworthiness is a key element in evaluating the worth of a study. These authors suggest that to assess a study’s trustworthiness, the researcher must consider 1) credibility, 2) transferability, 3) dependability, and 4) confirmability of the research.

2.3.8.1 Credibility

Credibility involves establishment of confidence that the study findings and interpretations are internally valid. Lincoln and Guba (1985:301) suggest seven techniques which a researcher can use to establish credibility: 1) prolonged engagement, 2) persistent observation, 3) triangulation, 4) peer debriefing, 5) negative case analysis, 6) referential adequacy, and 7) member-checking. The researcher made use of triangulation, peer debriefing, and negative case analysis.

Triangulation is a method that involves multiple data sources to either refute or concur with a particular proposition or state of affairs (Hesse-Biber & Leavy, 2011:51). Lincoln and Guba (1985:307) suggest that triangulation can be applied to theories as sources of data. As such, the researcher triangulated data pertaining to theories of insider espionage. Following the approach suggested by Yin (2018:196-197) on multiple-case studies, the researcher also performed triangulation by way of cross-case analyses involving four cases of insider espionage. The findings across the four case studies enabled the researcher to reach conclusions about the variables that act as predictors of insider espionage, and to validate the conceptual framework developed by the researcher.

Peer debriefing involves ‘exposing one's work to an independent peer in a matter of paralleling and analytic session for the purpose of exploring aspects of the inquiry that might otherwise remain only implicit within the inquirers mind’. Accordingly, the researcher worked on this project under the supervision of two highly experienced researchers who were available to discuss all aspects of the project and provided invaluable feedback.

The presentation of negative and discrepant information means that the researcher did not only capture and present information that supports a specific view, but also information that is negative or discrepant. The researcher has regarded such information as an opportunity for deeper understanding of the intricacies of insider espionage predictors. For example, such an opportunity arose while analysing the case of Oleg Gordievsky. Contrary to the researcher's early predictions (according to which mental disorders, substance abuse and addictions where the only factors that have a disinhibiting effect), there was no evidence of any of these in Gordievsky's case. Through the analysis of this case, it became evident that there are also other variables that can act as dis-inhibitors. Strong emotional reactions and certain personality characteristics could have the same effect. In an iterative process, this realisation was incorporated in the researcher's theory and conceptual framework.

2.3.8.2 Transferability

Lincoln and Guba (1985:300) proffer that transferability is the constructivist equivalent to the external validity criterion of neo-positivism. This criterion addresses the measures taken that allow the research findings to be applied to different subjects or situations. Lincoln and Guba (1985:316) suggest that while qualitative researchers cannot specify the external validity of their research, they can provide detailed information that allows interested researchers to apply the research results to a different situation. The latter orientation would enable such researchers to determine for themselves whether the transfer would be feasible.

2.3.8.3 Dependability

Dependability pertains to 'how the findings and interpretations could be determined to be an outcome of a consistent and dependable process' (Lincoln & Guba, 2013:105). A key concern related to dependability pertains to drift in the use of codes (Creswell & Creswell, 2018:202). The researcher utilised a codebook in which all the codes were defined in order to ensure the quality of the coding (see Annexure B). The researcher reviewed these definitions regularly to ensure that he continued to apply them consistently (Schreier, 2012:34). To shore up dependability claims, Lincoln and Guba (1985:316-318) suggest an audit, comparable with that of an audit in business or industry. The auditor would essentially have two tasks: 1) to examine the process with which the work was performed, and 2) to examine the 'product' for its accuracy. Such an audit has been conducted through the supervisors of the researcher.

2.3.8.4 Confirmability

Confirmability addresses the degree to which the findings and interpretations of the research can be traced back to the data collection, and whether they are the result of a dependable process of inquiry. The techniques for assessing confirmability include performing an audit, triangulation, and reflexivity (Lincoln & Guba, 1985:319; Lincoln & Guba, 2013:105). As outlined above, triangulation, peer debriefing, and an audit have been applied in this study. With a view to reflexivity, it is important for a researcher to reflect on the biases he or she might bring to the study (Creswell & Creswell, 2018:200). At the outset of the study, the researcher had certain preconceptions regarding one of the suggested predictors of insider espionage. Cases that were well known to the researcher prior to the commencement of this study included those of Geoffrey Prime and Robert Hanssen. Both individuals have been diagnosed with severe mental disorders.

Mental disorders can have a disinhibiting effect with respect to a subject's adherence to social and legal norms. Therefore, the researcher hypothesised at some point that all insider spies are afflicted with a mental disorder. It was important for the researcher to recognise this bias because this opened his thinking to the possibility of other factors than mental disorder, that have a disinhibiting effect. In the analysis of the four case studies, Oleg Gordievsky's case strongly suggested that his disinhibitions came from other sources (i.e. intense emotional state/affect combined with high ethical standards and specific personality structure).

2.3.9 Ethical considerations

Ethics is an important issue that should always be a point of consideration in any kind of research. Research documents should contain relevant information about the applicable ethical standards, and how the researcher intends to uphold them

(Denscombe, 2019:104). Resnik (2015:n.p.) asserts that there are several reasons for adherence to ethical standards by researchers. Ethical standards support essential aims of research, which include the acquisition of knowledge and truth, as well as the avoidance of error. Secondly, these standards promote values (e.g. accountability, mutual respect, and fairness), which are essential tenets of collaborative work. Thirdly, ethical standards ensure that researchers can be held accountable for the research work they perform. Fourthly, these standards help to build and maintain public confidence in support of research. Fifthly, the ethical standards support social values, such as social responsibility, human rights and justice (Resnik, 2015:n.p.).

Denscombe (2019:105) suggests that some types of research appear inoffensive and innocuous. The author cites studies in which documents are used that are already in the public domain as an example. He asserts, however, that even in such cases, ethical considerations should accompany the research because ethical standards do not only apply to parts of the research, but to the entire research process. This includes the way in which sources are selected, data are analysed, and findings are reported. Moreover, readers expect research to contain ethical considerations to have the assurance that the researcher has taken note of, and has applied the ethical standards relevant to the type of research conducted by the researcher.

In its 2016 revision of the Policy of Research Ethics, the University of South Africa informs the research community and the public of the standards to which this institution expects its researchers to adhere (University of South Africa, 2016). The researcher feels morally and ethically bound by the totality of these standards. Taking account of the specifics of this research project, however, the researcher emphasises those aspects in the UNISA policy that are particularly relevant to this study.

The researcher regards himself as a humanist. He considers the dignity of the individual as a fundamental tenet of humanity. In his view, this tenet must, without exception, always remain inviolable. He holds that individuals have fundamental rights, including those of autonomy, liberty, and personal growth. In a fair and just social and political system these rights always remain protected. From this philosophical and ethical stance, it follows that respect of the autonomy, rights and dignity of research participants is a *conditio sine qua non*, a condition without which research cannot seriously exist.

In the researcher's view, societies are enriched and can only reach their full potential if they support cultural diversity and pluralism. This, however, can only be achieved if the differences are not just tolerated, but unwaveringly respected and openly received. The cases that the study has reviewed are from different countries and cultural settings. The philosophical and ethical stance of the researcher demands a respectful and unbiased regard for cultural differences that is free of presumptions, prejudgements, and discrimination. The researcher upholds that this stance applies to any aspect of a well-functioning society and therefore, by definition, also applies to the research setting.

Research should serve to provide the welfare of people with a positive contribution (University of South Africa, 2016:11). The researcher suggests that insider espionage is a crime that endangers the safety and welfare of nations and organisations. The better this phenomenon is understood, the greater the likelihood of mitigating the risks associated with it. This research aims to offer a contribution in this regard.

In the researcher's understanding, justice is closely linked with the concepts of equity, fairness, and impartiality, without which justice cannot exist. In the research environment, this means that the benefits and risks of research should be distributed fairly (University of South Africa, 2016:11). Assuming the satisfactory completion of this project, the researcher will suggest that the work be published.

No harm should come to research participants or to people in general through research (University of South Africa, 2016:11). Denscombe (2019:104-105) asserts that individuals can be affected by the work of researchers in different ways, such as: 1) by data collected *from* individuals, 2) by data collected *on* individuals, and 3) by research *about* individuals. Given the design of this study and the nature of the findings, it is highly unlikely that harm could come to anyone. Moreover, this research will hopefully help to identify individuals who are vulnerable to becoming insider spies before they engage in such activity, thereby averting harm that might otherwise occur.

In the researcher's understanding, integrity implies the consistent and uncompromising adherence to ethical principles. The researcher is unequivocally committed to this form of conduct. Moreover, the researcher committed himself to transparency in all phases of the research. This includes honesty regarding his own limitations, competence, beliefs, values, and needs. Finally, the researcher assumes full responsibility for the research he has performed in this project and intends to perform in future projects. This refers to all aspects of academic honesty including the respect for intellectual property and, under all circumstances, the avoidance of plagiarism.

The research proposal associated with this study was reviewed by UNISA's Ethics Review Committee and has been found to be compliant with the university's ethical standards (see Annexure C). The researcher has adhered to these standards throughout this study.

2.4 CHAPTER SUMMARY

The present chapter has articulated the methodological framework of this study. In this discussion, the researcher has highlighted his reasoning for adopting a pragmatist worldview. This worldview lays the foundation for the selected research design. Research on insider espionage is *in status nascendi* (new and still in the state of becoming) and there is still more to be explored. For this reason, and in keeping with (Creswell, 2014:4), the researcher believes that a qualitative study is most appropriate. Given this choice of approach, the researcher has opted for the use of a case study design because it offers the greatest opportunity for in-depth analysis of events, activities, or processes that involve one or more individuals. A considerable amount of information related to insider espionage is not available in the public domain. The research population, sampling, data recording, analysis, and interpretation is, therefore, exclusively based on what is publicly available. Classified information of any sort was not considered in this study. Last, but certainly not least, the researcher has laid out his ethical views, which have consistently guided him through the various phases of this research project.

CHAPTER 3: EXPLORING THE VARIABLES OF INSIDER ESPIONAGE AND THE RELATIONSHIPS BETWEEN THEM

3.1 INTRODUCTION

Deterrence and detection of insider espionage are among the key responsibilities of defensive counterintelligence (Prunckun, 2019:25). However, counterintelligence is not particularly effective with either one. Deterrence does not appear to be working because there is a seemingly endless flow of new insider espionage cases every year. Detection is also not effective as the vast majority of insider spies are exposed through betrayal, rather than through the use of effective detection techniques (Charney, 2019:37).

In the past, the shortcomings of counterintelligence might have been attributable to a lack of focus on the causes of insider espionage. However, as established in the literature review in subsection 1.3.7, this began to change in the 1980s when the world witnessed a sharp increase in the number of insider espionage cases and researchers subsequently began to direct their attention towards this problem. The approaches that have since emerged address a variety of important aspects in an effort to explain how and why individuals cross the line. Despite this development, the problem of insider espionage is far from over. The end of the Cold War has also not changed this and with global tensions rising yet again, the problem of insider espionage has become an even greater concern (ERR News, 2022:n.p.; Herbig, 2017:17-20; Koot, 2022:n.p.; NFP, 2022:n.p.; Walker, 2022:n.p.). The need for an effective counterespionage programme is, therefore, as essential as ever.

As outlined in Section 1.3.13, while existing approaches to insider espionage provide important insights into why and how individuals become insider spies, each of the approaches only offer part of the mosaic: 1) none of the approaches capture the full range of variables that lead to insider espionage. 2) with respect to each of the factors, the constituent elements (variables) are only anecdotally addressed, and 3) the relationships between the factors, which jointly constitute a process leading to insider espionage, often remain unclear. The researcher has found that none of the existing approaches offer a comprehensive framework, which is an important shortcoming in current literature. As such, the researcher proposed to answer the following four questions:

> **Question 1**: What are the independent variables that are predictors of insider espionage (dependent variable) in the government and private sectors?
> **Question 2**: What are the relationships between the variables of insider espionage in the government and the private sectors?
> **Question 3**: How can the variables of insider espionage and the relationships between them be represented in an interdisciplinary conceptual framework that can serve to predict risks of insider espionage?
> **Question 4**: How can this interdisciplinary conceptual framework be applied to specific cases of insider espionage to identify the presence of predictors of insider espionage and thereby validate the conceptual framework?

In this chapter, the researcher will endeavour to answer the first two of the above-mentioned questions by systematically analysing the variables associated with insider espionage and the relationships between these variables. The study will serve to fill the many gaps that exist in current literature on insider espionage by drawing on existing literature in the fields of psychology, political science, security studies, economics, and psychiatry. Through this multidisciplinary approach, the researcher endeavours to lay the foundation for Chapter 4, which is necessary to answer the third question and its major focus on the researcher's development of an interdisciplinary conceptual framework that can serve to predict risks of insider espionage.

3.2 THEORETICAL CONSIDERATIONS

The development of a conceptual framework of insider espionage is one of the key contributions of this study. It is necessary to lay a solid theoretical foundation in order to develop such a conceptual framework and enabling analysis of the variables of insider espionage as instrumental in the current chapter. The researcher reasons that it is important to define the constitutes a theory prior to embarking on the analysis of the variables.

According to Urquhart (2013:5) a 'theory asserts a plausible relationship between concepts and sets of concepts'. Hollander (1967:55) suggests that 'a theory consists of one or more functional statements or propositions that treat the relationship of variables so as to account for a phenomenon or set of phenomena' (Jaccard &

Jacoby, 2010:28). In the view of Hage (1972:32) ‘Theory denotes a set of well-developed categories (themes, concepts) that are systematically interrelated through statements of relationship to form a theoretical framework that explains some phenomenon’. Strauss and Corbin (1998:15), define theory as ‘a set of well-developed concepts related through statements of relationship, which together constitute an integrated framework that can be used to explain or predict phenomena’. Jaccard and Jacoby (2010:28) define a theory as ‘a set of statements about the relationship(s) between two or more concepts or constructs’. Drawing on these definitions, the researcher holds that a theory is a framework that can be used to explain or predict phenomena and that consists of well-developed concepts that are systematically interrelated through statements of relationship.

Concepts are the building blocks for all thinking, regardless of whether that thinking relates to everyday matters or scientific inquiry. They are generalised (generic) abstractions that can be applied across a number of specific instances that are contained in universes of possibilities. Concepts possess no tangible reality in and of themselves but, as ideas regarding reality, they reflect what individuals deem to be real (Jaccard & Jacoby, 2010:11-12). A variable is one type of construct that is used in many scientific theories. With a view to a given (generic) construct, variables have or are composed of different ‘levels’ or ‘values’ (Jaccard & Jacoby, 2010:13). With this understanding, the concepts which theories contain may be variables.

Jaccard and Jacoby (2010:39-40) propose that for theory development, researchers basically engage in three processes: 1) generation of ideas and concepts, 2) refinement and focussing of concepts, and 3) clarification of the relationships between the concepts. The generation of ideas and concepts involves capturing the ‘mechanisms underlying the phenomena that you are trying to explain, without initially being too critical about the merits of those ideas’ (Jaccard & Jacoby, 2010:39). Literature reviews are subsequently a useful source to this end (Jaccard & Jacoby, 2010:47).

The literature review in Section 1.3 fulfilled the purpose of the first process by generating ideas and concepts. It is evident that each approach to insider espionage offers a part of the mosaic, but that none provides the complete picture as to why or how someone becomes an insider spy. Nevertheless, in Section 1.3.13, the researcher found that while the variables contained in these approaches vary considerably, they could all be captured by one of five factors (concepts). Figure 3.1 depicts these five factors (i.e. triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors). The figure represents the overarching framework that the researcher has used as a basis for the detailed analysis he has conducted in the following subsections. In this sense, these five concepts constitute an initial approximation of the variables of insider espionage.

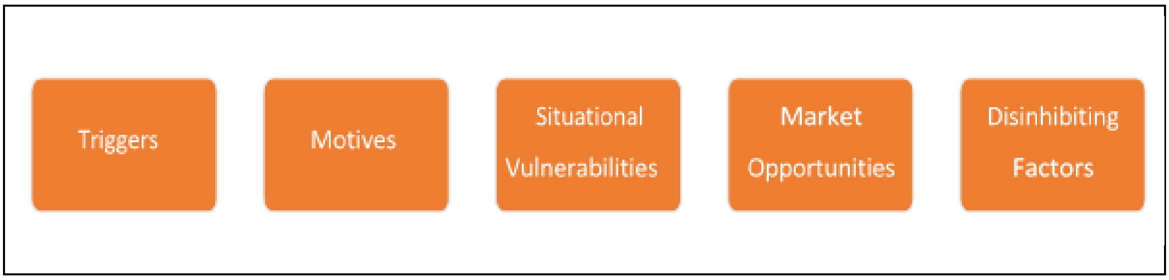


Figure 3.1: Factors of insider espionage
(Source: Developed by the researcher)

The second process of theory development - the refinement and focussing of concepts - involves the formal characterisation of the process of specifying conceptual definitions based on the work performed in the first process (Jaccard & Jacoby, 2010:75) and the third process, the clarification of the relationships between the concepts, involves the explanation of the relationships between the concepts (Jaccard & Jacoby, 2010:91). Based on this understanding of how a theory is developed, the researcher proposes to refine and focus the five concepts (factors) depicted in Figure 3.1 and to clarify the relationships thereof.

The researcher regards this as an essential step because while the five factors depicted in the figure offer a useful first approximation in the development of a conceptual framework, the factors are merely five labels unless defined and understood with respect to their constituent variables. In the researcher’s view, this necessitates the systematic analysis of all relevant variables pertaining to each of the factors rather than the reliance on anecdotal observations which are typical of the approaches found in current literature.

By providing a systematic analysis in the following subsections, the researcher aims to remedy a major shortcoming of current literature as outlined in Section 1.3.13 by filling the existing gaps, by realigning the variables and clarifying how they relate to the process of becoming an insider spy in a coherent structure. It is through these measures that the researcher will refine and focus the concepts and elaborate the relationships in the meaning of Jaccard and Jacoby (2010:91), and thus lay the foundation for the conceptual framework of insider espionage which the researcher will develop in Chapter 4 of this study. In this regard, the researcher aims to provide a contribution to existing literature by offering solutions to the shortcomings in current approaches.

3.3 TRIGGERS OF INSIDER ESPIONAGE

As suggested in Section 3.2, the first factor to examine in the context of insider espionage is that of the trigger (see Figure 3.1). From a conceptual premise, it seems appropriate to consider the trigger first because it catalyses the process of becoming an insider spy. Heuer (2001:n.p.) asserts that the decision to commit espionage is generally preceded by an individual's personal or professional life stresses that are so severe and cause the individual to become a spy. He also points out that triggers can take various forms. Wilder (2017:20) suggests that states of crises can act as triggers. Herbig (2008:42) suggests that life events in general can be triggers and Moore et al. (2016:1), focus specifically on negative organisational incentives as triggers. While these three viewpoints provide a sense of the vast difference immanent in triggers, they also suggest a need for some form of reconciliation. This is the focus of the next two subsections.

3.3.1 Events and situations acting as triggers

Espionage can be triggered by a myriad of events or situations. Examples include 'financial problems combined with an available opportunity for illegal gain; failure to compete effectively with one's peers; perceived injustice at the hands of an employer or supervisor; termination from a job under circumstances that prompt resentment; rejection or betrayal by a spouse or other close family member' (Heuer, 2001:n.p.).

In a review of 173 cases of insider espionage, Herbig (2008:42), draws on the comprehensive list of life-events advanced by Ross and Mirowsky (1979:176-177) and relates these events to acts of insider espionage. Table 3.1 lists the life events advanced by Ross and Mirowsky (1979:176-177) that Herbig (2008:42) used in her research. Based on this list, Herbig was able to identify 57 cases (about 33%) in which the offenders encountered a life event some months prior to engaging in insider espionage. Herbig (2008:42) suggests that the life events played a role in the individuals' decisions to become spies. The author also points out that the number of cases preceded by life-events could possibly be more than the 57 cases initially identified. Data on such events in the lives of insider spies are often missing from open sources. Typically, it is only in the most damaging cases that the surrounding circumstances are the subject of in-depth journalistic or historic research (Herbig, 2008:42).

Table 3.1 Undesirable and desirable life events

Undesirable Life-events	**Desirable Life-events**
1. School problems 2. Relocation to a worse neighbourhood 3. Widowed 4. Divorced 5. Separated 6. Trouble with in-laws 7. Serious physical ailment 8. Serious accident or injury 9. Death of next-of-kin 10. Stillbirth 11. Frequent minor illnesses 12. Mental instability 13. Death of a pet 14. Demotion to lesser job responsibilities 15. Retrenchment (temporarily) 16. Failed business 17. More than a month's employment 18. Expulsion from work 19. Financial deterioration 20. Court appearance 21. Correctional detention 22. Experience of arrest 23. Litigation 24. Losing a driver's licence	1. Attended school or began training programme 2. Graduated from school or training programme 3. Moved to a better neighbourhood 4. Built a new house 5. Major remodelling of house 6. Engaged 7. Married 8. First child's birth 9. Adopting a child 10. First work experience 11. Promotion to more job responsibilities 12. Expanded business 13. Significant work success 14. Improved financial status

(Source: Ross & Mirowsky, 1979:176-177)

While lacking in-depth research might explain the absence of data regarding life events in the periods leading up to the acts of espionage, an alternative explanation could be that triggers are simply not always as dramatic as those contained in the list of Ross and Mirowsky (1979:176-177). This is illustrated in the cases of James Hall, Clayton John Lonetree, and William Kampiles. Hall was a U.S. Army Warrant Officer who, by his own admission, committed espionage out of greed rather than financial need. He was not faced with financial hardship and only driven by the desire to attain a more affluent lifestyle than that which his income allowed (Defense Personnel Security Research Center, 2009:18-19). Lonetree was a Marine Corps security guard at the US Embassy in Moscow who was trying to impress his Russian girlfriend when he provided her with US government secrets unaware of the fact that she was a KGB operative (Defense Personnel Security Research Center, 2009:34).

Kampiles was a CIA office worker who aspired to become a field agent. Upon the realisation that his qualifications fell short of the requirements for the advancement he desired, he devised a plan to prove that he could be an effective operative even without the required qualifications. He stole a classified document from the CIA, sold it to a foreign intelligence officer and reported his actions to CIA managers hoping to impress them with his skills as a field operative. Instead of the outcome Kampiles hoped, he was arrested, tried, and imprisoned (Defense Personnel Security Research Center, 2009:27). While the mentioned individuals' respective circumstances were evidently important enough to trigger their acts of espionage, none of the situations would classify as life-events in the meaning of Ross and Mirowsky (1979:176-177).

The case of William Kampiles also serves to illustrate another important point, namely that diminished job satisfaction can act as a trigger that eventually leads to insider espionage (Defense Personnel Security Research Center, 2009:27). Branham (2004:12) points out that there are many events and situations in the work setting that can act as triggers and cause employees to become disengaged. These triggers are listed in Table 3.2, which illustrates how broad the range of potential triggers in the workplace are. Such triggers may include being passed over for a promotion, realising that the job is not as promised, or the hiring boss being replaced by a new boss who the employee does not like. While these may not be life-events, such circumstances can become the ‘‘last straw’’ that trigger a gradual build-up of employee frustration, eventually leading to a breaking point, and finally motivating some form of counterproductive work behaviour without being noticed by the employee’s supervisor (Branham, 2004:12).

Table 3.2: Work-related triggers causing employee disengagement

1. Being passed over for promotion
2. Unfulfilled job promises
3. Possibilities of unwelcome transfer
4. Replacement of a liked boss
5. Assigned to new geographic area
6. Directed to unethical conduct
7. Noting unethical company practices
8. Being underpaid compared to colleagues
9. Expected promotion remaining unfulfilled
10. Realisation of unacceptable personal behaviour
11. Unexpected external job offer
12. Pressured to commit unreasonable personal or family sacrifice
13. Being asked to perform a menial duty (e.g., run a personal errand for the boss)
14. Unreasonable and petty expression of authority
15. Denial of family leave request
16. Denial of transfer request
17. Close colleague quitting or being fired
18. Disagreement or conflict with co-worker or the boss
19. Surprising low performance rating
20. Surprisingly low pay increase or no pay decrease

(Source: Branham 2004, 12-13)

The work-related triggers proposed by Branham (2004:12) all point to some form of conflict between the expectations of the individual and the actions of the organisation. According to Dlugos (1981:657-658) and Dorow (1982:151), such expectations can be clustered into five categories: 1) income, 2) job security, 3) work requirements, 4) professional growth and participation, and 5) social conditions. Conflict occurs either when an employee’s wishes are not sufficiently satisfied with respect to income, job security, professional growth and participation, or social conditions or when the employer makes excessive demands in terms of work requirements.

Until now, the discussion suggests that there are many kinds of events and situations that can act as triggers to insider espionage: states of crises, exceptional positive and negative life events, negative organisational incentives, work conditions, as well as events or situations that others would consider undramatic (Branham, 2004:12; Dlugos, 1981:657-658; Dorow, 1982:151; Herbig, 2008:42;

Heuer, 2001:n.p.; Wilder, 2017:20). Essentially, any stimulus (i.e. event or situation) that elicits a reaction is a trigger (American Psychological Association, 2020:n.p.). However, it is important to recognise that not every stimulus elicits a reaction. This prompts the question of what accounts for the differences in individual responses. In the researcher’s view, this can best be explained by exploring the predispositions of individuals.

3.3.2 Analysis of predispositions

Events and situations can have vastly different effects on people. Faced with the same stimulus, one person might be aroused and, therefore, be motivated to take an action while another person regards the same stimulus with complete indifference and, therefore, be inclined to ignore it. For an event or situation to become a trigger, it must in some way affect a person’s predispositions, which is defined as tendencies to maintain distinct attitude and acting in specific manner. They can relate to a person’s 1) needs, 2) beliefs, 3) values, or 4) ideology (Deckers, 2016:369; McClelland, 1987:6; Rokeach, 1968:113).

Needs are predispositions that are ‘essential for an individual’s adjustment, integrity and growth’ (Vansteenkiste, Ryan & Soenens, 2020:1). They directly relate to an individual’s personal history and occur both, as enduring traits, and as temporary states (Deckers, 2016:202-203). The satisfaction of a need is conducive to, and sometimes essential for, an individual’s wellbeing and frustration of a need can bring about a host of adverse reactions (Vansteenkiste et al., 2020:1). Needs manifest themselves when they are not satisfied, and can occur through a process of reintegration, in which an event or situation raises an individual’s awareness of a discrepancy between that which the individual desires and that which is a reality (Deckers, 2016:202; McClelland, 1987:7).

The centrality and role of needs in determining human behaviour necessitates that the question of a clearly articulated definition should be addressed. Haggbloom, Warnick, Warnick, Vinessa, Yarbrough, Russell, Borecky, McGahhey, Powell, Beavers and Monte (2002:139 & 146) inform that the work of Abraham Maslow (1970/1987) continues to rank among the most frequently referenced works in response to this question. According to Maslow, human needs can be categorised as physiological, safety, belongingness and love, self-esteem, and self-actualisation needs; with physiological needs as the most basic. The latter needs are driven by homeostasis or states like hunger, thirst, fatigue, and sexual desire (Maslow, 1970/1987:57-59).

Safety needs include security, protection, and stability as well as freedom from fear, anxiety, and chaos. They also include needs for structure, order, and laws that protect one’s interests (Maslow, 1970/1987:60). Needs for belongingness and love involve giving and receiving affection that may be experienced in friendship, companionship, or family life. The need for belongingness and love can be exacerbated by feelings of loneliness, ostracism, rejection, and the absence of friendship (Maslow, 1970/1987:62).

Self-esteem relates to the notion that people generally have for a positive self-image. This involves aspects like strength, achievement, adequacy, mastery and confidence including a good reputation, enjoying status, receiving positive attention, and having a sense of self-importance and dignity (Maslow, 1970/1987:63). Self-actualisation refers to the need for the individual to live up to his or her potential and achieving a state of self-fulfilment. The needs vary in respect of the individual’s preference within his or her own frame of reference (Maslow, 1970/1987:64).

The cases of Richard W. Miller and Svetlana Tumanova illustrate how events or situations combined with the specific needs of the individuals could lead to a chain of events that trigger insider espionage. Miller was an FBI agent who became sexually involved with a married female KGB agent in Los Angeles before providing her with classified FBI documents. He was ensnared in a classic ‘honey trap’ operation in which his sexual needs were exploited to gain access to classified information (Defense Personnel Security Research Center, 2009:37-38). Estonian born Svetlana Tumanova was a secretary who began working for the US Army Foreign Language Training Center in Munich, Germany after her naturalisation as a U.S. citizen. Foreign intelligence operatives coerced Tumanova into committing espionage by threatening the safety of her parents who at the time lived in Estonia (Defense Personnel Security Research Center, 2009:58). In both cases, the individuals were faced with situations that related to their needs. Miller had the need to engage in sexual exploits (a basic human need) and Tumanova had the need to provide for the safety of her parents. Thus, both circumstances acted as triggers for motives that culminated in acts of espionage.

Similar to needs, beliefs are important predispositions that may cause events or situations to become triggers. Beliefs play a central role in our cognitive processes because they reflect what we think is true or not (Cottam, Dietz-Uhler, Mastors & Preston, 2010:131-132; McClelland, 1987:518-519). Beliefs contain the ‘cognitive components that make up our understanding of the way things are’ (Glynn, Herbst, O'Keefe & Shapiro, 1999:104). For Rokeach (1968:113), “a belief is ‘any predisposition, conscious or unconscious, inferred from what a person says or does, capable of being preceded by the phrase ‘I believe that …’’. Additionally, beliefs reflect the attributes that an individual associate with an event or situation (Cottam et al., 2010:131-132).

When beliefs are organised in a cluster, we speak of a belief system (Cottam et al., 2010:131-132). A belief system consists of the ‘total universe of a person's beliefs about the physical world, the social world, and the self’ (Rokeach, 1968:123). Each belief system is characterised by three components: the cognitive, the affective, and the behavioural. The cognitive component consists of the individual’s knowledge of an object or situation with certainty. The affective component is able to arouse an emotional response to the event or situation when conditions are most suitable. The behavioural component refers to the notion that beliefs are response dispositions with varying threshold levels that can, under suitable conditions, trigger certain behaviours (Rokeach, 1968:113-114).

The object of a belief is characterised as false or true, bad or good, or desirable or undesirable. The first form of belief is referred to as a ‘descriptive’ belief (‘I believe that the 16:05 train will only stop at Southampton’). The second is an ‘evaluative’ belief (‘I believe that the train is a good mode of transportation because it is reliable and comfortable’). The third form of belief is ‘prescriptive’ (‘I believe that the train should not just stop at Southampton but, for the sake of convenience, also at Portsmouth’) (Rokeach, 1968:113).

Prescriptive beliefs can be specific concerning an object or situation, as in the preceding train example, or can be unspecific and global (‘Life should be as comfortable as possible; convenient infrastructures are helpful in this regard'). Prescriptive beliefs that are global and unspecific concerning an object or situation are referred to as values that reflect general terms of wishes and ambitions (Cottam et al., 2010:132). According to Kluckhohn (1951:389), a 'value is a conception, explicit or implicit … of the desirable which influences the selection from available modes, means, and ends of action'. Values are global beliefs that 'transcendentally guide actions and judgements across specific objects and situations' (Rokeach, 1968:160). Depending on their importance to the individual, values may be intense beliefs that contain strong emotional components (Cottam et al., 2010:7). For this reason, values can be 'determinants of virtually all kinds of behaviour that could be called social behaviour' (Rokeach, 1973:24).

Values serve two important functions. They serve as standards that allow us to judge a given behaviour as being praiseworthy or blameworthy (Dorow, 1981:677-678; Hayes, 1994:604). They also motivate behaviour that individuals strive to live up to, and 'act in accordance with them if [they] possibly can' (Hayes, 1994:604). Values guide actions in various ways, such as: prompting specific standpoints concerning political issues; predisposed to embracing or rejecting certain ideologies; providing the language with which to describe one's own prescriptive beliefs; evaluating (judging, praising, or rebuking) actions; providing the language with which to compare oneself with others; providing the language with which to persuade others; and allowing individuals to rationalise their own actions (Dorow, 1981:677-678). Figure 3.3 below provides an overview with respect to existing values. According to Rokeach (1979:62-65), there are two common categories: Terminal values and instrumental values. The final goal or desired result is referred to as a terminal value. Beliefs regarded as instrumental values pertain to 'desirable modes of behaviour that are instrumental to the attainment of desirable end- states' (Rokeach, 1979:48).

Table 3.3: Terminal and instrumental values

Terminal Values	Instrumental values
• a comfortable life • an exciting life • a sense of accomplishment • a world at peace • a world of beauty • equality / justice • family security • freedom • happiness • inner harmony • mature love • national security • pleasure • salvation • self-respect • social recognition • true friendship • wisdom	• ambitiousness • broadmindedness • capability • cheerfulness • cleanliness • courage • leniency • helpfulness • honesty • imagination • independence • logical thinking • lovingness • obedience • politeness • responsibility • self-control

(Source: Rokeach, 1979:62-65)

Ideologies account for a large part of our understanding of espionage. Levchenko (1988:106) describes ideology as one of the most important reasons why individuals turn to espionage. According to a study by Herbig (2017:41) a quarter of the individuals who committed espionage without financial motivations did so for reasons of ideology or divided loyalties. In the field of psychology, ideology is defined as an organisation of religious, political, or philosophical beliefs that are ‘more or less institutionalized or shared with others’ (Rokeach, 1968:123-124). In political science, ideology is defined as a ‘more or less coherent set of ideas that provides the basis for organized political action, whether this is intended to preserve, modify, or overthrow the existing system of power’ (Heywood, 2017:10).

Heywood (2017:10) asserts three characters common in : 1). They offer an account of the existing order, 2) they provide a model for a ‘good society’ for the future, and 3) they map a course how to transition from the existing order to the desired future. These features respectively correspond with descriptive, evaluative, and prescriptive beliefs within a belief system (Rokeach, 1968:113).

Beliefs, values, and ideologies have played a role in the insider espionage cases of Oleg Antonovich Gordievsky and Monica Elfriede Witt. Gordievsky was an intelligence officer with the KGB who was a convinced communist but disagreed with the heavy-handed measures that the Soviet Union took to secure its interests which included crushing the Hungarian Uprising in 1956 and the Prague Spring liberalisation movement in 1968. Disaffected by these measures, which violated his own liberal values, Gordievsky offered his services to spy for the British MI6 from 1974 until his defection in 1985 (Gordievsky, 2018:213). Monica Elfriede Witt was an intelligence officer with the US Air Force and later defence contractor working for Booz Allen Hamilton. Witt converted to the Muslim faith, eventually became radicalised and critical of the US government, and defected to Iran in 2013 where she disclosed top-secret information that she had gathered prior to her defection (Blinder, Turkewitz & Goldman, 2019:n.p.; United States District Court for the District of Columbia, 2018:n.p.).

3.3.3 Factor summary

Triggers are stimuli (events or situations) that elicit reactions and prompt action (American Psychological Association, 2020:n.p.). States of crises, negative organisational incentives, and significant life events can act as triggers (Herbig, 2008:42; Moore et al., 2016:1; Wilder, 2017:20). However, the cases of James Hall, William Kampiles, and Clayton John Lonetree show that events or situations that are less drastic could also become triggers (Defense Personnel Security Research Center, 2009:18-19, 27 & 34). Events and situations affect people differently. A given event or situation may arouse one person and thus trigger a motivation process while another person would regard the same stimulus with indifference and therefore, not be motivated by it. An event or situation acts as a trigger by stimulating an individual’s needs, beliefs, values, or ideology (Deckers, 2016:369; McClelland, 1987:6; Rokeach, 1968:113). It is, therefore, the event or situation combined with the individual’s predisposition and not the event or situation alone that triggers a motivation process.

3.4 MOTIVES OF INSIDER ESPIONAGE

Inferring from the analytical framework advanced in Section 3.2, the second factor to consideration is motive. The philosopher Arthur Schopenhauer (1788–1860) was one of the first to speculate on the relationship between motives and behaviours. Schopenhauer believes that ‘human action is always induced by a motive or counter-motive, whichever is stronger’ (Schopenhauer, 1841:5-6). Likewise, modern-day psychologists consider motivation to be a key concept in understanding the determinants of human behaviour (Deckers, 2005:194; Griggs & Jackson, 2020:177; Nolen-Hoeksema, Frederiksen, Loftus & Lutz, 2014:343 & 347). According to Griggs and Jackson (2020:177) motivation is the ‘set of internal and external factors that energise our behaviour and direct it toward goals’. Nolen-Hoeksema et al. (2014:343), define motivation as a ‘condition that energises behaviour and gives it direction’.

Motivation is a process, which involves making a choice about a need, belief, value, or ideology. It is through this process that motives are formulated. Motives relate to an individual’s ‘internal disposition to be concerned with and [to] approach positive incentives and avoid negative incentives’ (Deckers, 2016:2). Motivation psychologists sometimes use a push-pull metaphor to explain this concept. Hence, it is an unfulfilled need or unsatisfactory state that pushes the individual towards some form of resolution. Incentives are the counterparts of motives, through which, needs are fulfilled or desirable states are achieved. Incentives therefore have a pull effect by drawing the individual towards a specific solution (Deckers, 2016:2).

Once activated by triggers, motivation processes consist of 1) an appraisal by the individual as to the positive or negative impact of the trigger, 2) an emotional reaction proportionate with the appraisal of the trigger, and 3) a degree of action readiness based on the intensity of the emotional reaction (Deckers, 2016:369-370). Motivation is thus a process that is triggered by an event or situation and consists of a sequence involving an appraisal, an emotional response, and a degree of action readiness. It is through this process that a need, belief, value, or ideology pushes the individual to some form of action (Deckers, 2016:369-370).

The motivation process can be illustrated with the case of the former FBI officer Robert Hanssen who volunteered his services to spy for the Soviet Union and later for its successor, the Russian Federation. Hanssen had a large family which he was finding increasingly difficult to support on his FBI salary. His need for financial security presented an increasing strain. Hanssen had ambitions to progress within the hierarchy of the FBI, which would have improved his financial situation. His efforts to advance remained unsuccessful and his career stagnated while colleagues with less seniority progressed within the organisation's hierarchy. In his appraisal, Hanssen was in an extremely negative situation that was unfair, not realising that it was, in fact, his own awkward character that had been preventing him from achieving his goal. Being denied the promotions brought on increasingly emotional responses, leading to reports of enragement each time he was yet again blocked in his advancement. Hanssen could no longer cope with his career situation, and sought other means of reprieve (Vise, 2002:n.p.).

The case of Robert Hanssen illustrates how a given event or situation (denial of career advancement and financial stability) can lead to an extremely negative appraisal (perception of profoundly unfair treatment) and thus evoke an emotional reaction (rage), which finally leads to a high level of action readiness (seeking alternative means of recognition and financial security). However, it is also important to recognise that when comparing individuals in the same situation, a given stimulus can produce very different results. While Hanssen was outraged because of his lack of career development and eventually chose to become a spy, most personnel who have access to classified information and could abuse their privilege to commit espionage choose not to do so, even if their professional or personal circumstances could offer a motive (Heuer, 2001:n.p.). To understand why some individuals become spies while most others do not, the researcher argues the importance of understanding appraisals, emotions, and action readiness in the motivation process.

3.4.1 Appraisal

As noted already in the preceding section, people respond differently to similar events and situations. Financial worries, for example, cause some people to cross the boundary of legality, while others dare not entertain or act on the idea (Heuer, 2001:n.p.). Appraisal theories explain such differences. These theories hold that 'emotions are elicited by evaluations (appraisals) of events and situations' rather than by the events and situations themselves (Roseman & Smith, 2001:3). Appraisal theorists regard the appraisal as an intervening process that follows an event or situation and precedes the emotional response to that event or situation. In this view, it is the appraisal that determines the emotional response to the event or situation (Roseman & Smith, 2001:3).

According to Smith and Ellsworth (1985:817-818, 822 & 829), there are five dimensions with which individuals appraise events and situations:

- **Pleasantness** - The dimension pleasantness and unpleasantness, refer to the amount of comfort (pleasure) or discomfort (pain) that an event or situation causes to the individual. Evaluations based on pleasantness tend to be so immediate in relation to an event that some researchers disregard them as cognitive evaluations but rather as evaluations that precede cognition (Smith & Ellsworth, 1985:818).
- **Anticipated effort -** Anticipated effort refers to the extent to which individuals will exert themselves to deal with an event or situation (Smith & Ellsworth, 1985:822). While challenging events or situations are synonymous with increased levels of anticipated effort, while on the other hand, monotonous situations are linked with low levels of effort. When individuals regard events or situations as adverse, they expend some effort to ameliorate such efforts (Smith & Ellsworth, 1985:817-818).
- **Certainty** - Certainty relates to the individual’s understanding of the circumstances surrounding an event or situation and the predictability of related outcomes (Smith & Ellsworth, 1985:822). Low levels of certainty correlate with emotions such as hope and fear whereas high levels are associated with happiness, as is with boredom (Smith & Ellsworth, 1985:829).
- **Attentional activity** - Attentional activity is an appraisal dimension that addresses the extent to which events or situations meet or violate the expectations of the individual, and thus either demand attention or can be ignored (Smith & Ellsworth, 1985:817-818). Events and situations that are high in attentional activity can be appraised as challenging, thus, providing a sense of frustration and contempt along with interest. Events and situations that require low levels of attentional activity are, above all, associated with boredom whereas intermediate levels of attentional activity providing emotions of surprise, hope, and happiness (Smith & Ellsworth, 1985:829).
- **Responsibility and control -** Responsibility refers to the extent to which the individual or someone or something other than the individual brought about a

given event or situation. Control refers to the extent to which the individual can influence what is happening in a given event or situation (Smith & Ellsworth, 1985:829).

According to Smith and Ellsworth (1985:835), any of these dimensions can influence the emotional reaction of the individual. The dimensions allow the individual to broadly distinguish events as being positive or negative (desirable or undesirable) and its importance to the individual. Mildly negative or mildly positive events or situations may remain under the threshold that would otherwise invoke an emotional reaction. The person would respond with indifference. If, however, the appraisal is above the threshold, an emotional reaction is likely to follow (Smith & Ellsworth, 1985:835).

3.4.2 Emotional reactions

Keltner and Shiota (2003:89) proffer that an emotion is a ‘universal, functional reaction to an external stimulus event, temporarily integrating physiological, cognitive, phenomenological, and behavioural channels to facilitate a fitness-enhancing, environment-shaping response to the current situation’. Emotions integrate cognitive, and behavioural elements so as to facilitate an optimal response. Subject to the trigger, the response may be one of approach, avoidance, or inaction (Deckers, 2016:339; Keltner & Shiota, 2003:89). Deckers (2016:367-368) similarly posits that emotions unfold from events and situations (stimulus changes) that in some way affect the individual. Once triggered, emotions push the individual to respond with a goal directed action (Deckers, 2016:367-368). This is a key point as it implies that if the emotional reaction of an individual is known, the purpose and possibly the type of action can be anticipated.

There are many emotions to which individuals respond to events and situations. Psychologists have, therefore tried to bring some form of order to the wide array of possible emotional responses by identifying basic emotions to which other emotions are associated. The basic emotion of happiness, for example, can be associated with a range of other emotions like extasy, euphoria, joy, carefreeness, and light-heartedness (Deckers, 2016:342-343). Compiled by Ortony and Turner (1990:316), Table 3.4 provides an overview of categories that psychologists have developed to identify basic emotions. Taking account of the most frequently cited basic emotions in this table, majority can be clustered into four categories:

- Cluster 1: Anger, which includes rage, aversion, hate, and disgust (n=20);
- Cluster 2: Sadness, which includes sorrow, shame, grief, dejection, and despair (n=10);
- Cluster 3: Fear, which includes terror, anxiety, distress, and panic (n=15); and
- Cluster 4: Happiness, which includes joy, elation, desire, love, and tenderness (n-14).

Table 3.4: Categories of basic emotions

Arnold (1960)	Anger, aversion, courage, dejection, desire, despair, fear, hate, hope, love, sadness
Ekman, Friesen, & Ellsworth (1982)	Anger, disgust, fear, joy, sadness, surprise
Frijda (personal communication, September 8, 1986)	Desire, happiness, interest, surprise, wonder, sorrow
Gray (1982)	Rage and terror, anxiety, joy
Izard (1971)	Anger, contempt, disgust, distress, fear, guilt, interest, joy, shame, surprise
James (1884)	Fear, grief, love, rage
McDougall (1926)	Anger, disgust, elation, fear, subjection, tender- emotion, wonder
Mowrer(1960)	Pain, pleasure
Oatley & Johnson-Laird (1987)	Anger, disgust, anxiety, happiness, sadness
Panksepp (1982)	Expectancy, fear, rage, panic
Plutchik (1980)	Acceptance, anger, anticipation, disgust, joy, fear, sadness, surprise
Tomkins (1984)	Anger, interest, contempt, disgust, distress, fear, joy, shame, surprise
Watson (1930)	Fear, love, rage

(Source: Ortony & Turner, 1990:316)

It is the researcher's view, that these clusters are important for the present analysis due to emotional responses that are known to have played a role in prompting individuals to commit espionage as illustrated in the following sub-sections.

3.4.2.1 Cluster 1: Anger

Anger was instrumental in the case of former Lockheed Corporation engineer John Douglas Charlton. Charlton was incensed over being pushed out of Lockheed under an early retirement program and stole classified information which he intended to sell as an act of revenge (Sneiderman, Slater & Glionna, 1995:n.p.). In a different case, contempt, and disgust over the Soviet Union's handling of the Hungarian Uprising and the Prague Spring drove KGB Colonel Oleg Gordievsky to offer MI6 his services as a spy (Gordievsky, 2018:213; MacIntyre, 2018:58).

3.4.2.2 Cluster 2: Sadness

Saddened by his lack of career prospects at the CIA, William Kampiles devised a plan with which he hoped to impress CIA management by stealing a classified document from the CIA and selling it to a foreign intelligence agency. Kampiles believed that would demonstrate to the CIA his ability to work as a field operative (Defense Personnel Security Research Center, 2009:27).

3.4.2.3 Cluster 3: Fear

Fear of financial woes was reportedly a driver in the recent case of Italian navy captain Walter Biot who sold secrets to Russia in exchange for money (BBC, 2021:n.p.).

3.4.2.4 Cluster 4: Happiness/Joy

Desire was reportedly a key factor in the case of former FBI agent, Richard W. Miller who was ensnared in a classic 'honey trap' operation by a foreign operative. Unaware of her affiliation, he shared classified information with her (Sulick, 2013:125-126; Thornton, 1984:n.p.).

It is noteworthy, however, that the emotional responses did not engender immediate acts of espionage. They merely triggered the willingness to initiate some form of action (i.e., action readiness). Emotional reactions lay the foundation for action readiness.

3.4.3 Action readiness

Action readiness is the third element in the motivation process. Deckers (2016:359) describes action readiness as 'a state of preparedness to execute a particular kind of behaviour'. Action readiness reflects the individual's preparedness to engage in some adaptive action that is triggered by an emotion. However, it does not necessarily follow that an action will be taken. Action readiness may prevail without becoming manifest through action until the time or occasion is there for the action readiness to manifest itself in situation-adapted actions. Depending on the circumstances, such readiness may linger indefinitely (Deckers, 2016:359).

An important characteristic of emotions is that they motivate behaviour towards specific ends. Humans strive towards many things that result in the feeling of gratification, and avoid those that cause discomfort or pain (Deckers, 2016:388). Action readiness is ‘a state of preparedness to execute a particular kind of behaviour’ that is appropriate with respect to the emotion that the individual experiences (Deckers, 2016:359).

Situations that engender joyfulness and happiness may include social interactions, and are likely to motivate consummatory behaviour (Izard, 1993:68). If a situation (stimulus) causes an individual to feel fearful, the individual’s goal will likely be to escape from the impending danger (Izard, 1993:82 & 85-86). Anger is often the result of a blocked goal. If a situation causes someone to be angry, the individual will likely be motivated to remove the obstacle that is blocking his or her goal. Each emotion is associated with certain goals, which in turn, determine how individuals act with respect to the stimulus (Deckers, 2016:389). Table 3.5 provides an overview of the emotions that individuals may experience, the goals that are associated with these emotions, and the actions that they are likely to take.

Table 3.5: Goals of emotions and actions they motivate

Emotion	Goal	Action Tendency
Joy/happiness	To reward goal achievement To motivate consummatory behaviour (eating, sex)’ To maintain social interaction	Any instrumental behaviour achieving goals leading to consummatory behaviour, or maintaining interactions.
Sadness	To seek help to render harm or loss easier to bear To bring people together To scrutinize the cause of sadness’ To promote disengagement from the lost object/person’	Signalling others to help
Fear	To motivate escape from danger To focus attention on stimulus for danger	Avoid, escape, freeze or immobility depending on the stimulus and situation

Emotion	Goal	Action Tendency
Anger	To motivate to remove obstacle blocking goal To discourage another's anger or aggression	Actual removal of goal-blocking obstacle
Disgust	To maintain clean environment for survival To keep person from harmful substances	Escaping or avoiding the disgusting object
Shame	To maintain respect of others, restore self-esteem'	Escaping or avoiding situation and people
Guilt	To undo effect of one's misdeeds	Make amends, apologising
Embarrassment	To restore harmonious social relationships	Withdrawal, apology, providing explanation
Pride	To reinforce successful achievement of socially valued behaviours	Acts of altruism. treat others well

(Source: Deckers, 2016:389)

The distinction between action readiness and the action itself is perhaps best illustrated in the cases of Aldrich Ames and Oleg Gordievsky. Ames was fearful of being left by his wife and believed that providing her with a luxurious lifestyle would dissuade her from leaving him. However, his income was insufficient to meet this objective. He had considered robbing a bank, but ultimately resorted to committing espionage (Earley, 1997:136). In the case of Gordievsky, the Soviet invasion of Czechoslovakia during the Prague Spring pushed him to the breaking point. Gordievsky was so appalled by the military operation that he was determined to act against the Soviet Union. Before considering espionage, he also considered other types of action. One such action was to subvert the Soviet Union by distributing underground reports in Russia that would shed a positive light on NATO and the West (Gordievsky, 2018:213-214). In both these cases, the willingness to act followed an emotional reaction and preceded the decision of what concrete action to take.

3.4.4 Factor summary

Drawing on the analytical framework advanced by the researcher in Section 3.2, the second factor to consider is that of the motive. Motivation is a key concept in understanding what determines human behaviour (Deckers, 2005:194; Griggs & Jackson, 2020:177; Nolen-Hoeksema et al., 2014:343 & 347). Motivation is the ‘set of internal and external factors that energise our behaviour and direct it toward goals' (Griggs & Jackson, 2020:177). It is through the motivation process that a motive is formulated. A motive is a need, belief, value, or ideology that 1) is stimulated by an event or situation, 2) is appraised by the individual as being positive or negative, 3) is important enough to the individual to elicit an emotional reaction, and 4) initiates an individual's action readiness (Deckers, 2016:369-370).

Appraisals involve determining the extent to which the individual is positively or negatively affected by an event or situation. Appraisals take five dimensions into account: pleasantness, anticipated effort, certainty, attentional activity, responsibility and control (Smith & Ellsworth, 1985:817-818, 822 & 829). Appraisals determine the emotional reaction of the individual to an event or situation (i.e., anger, sadness, fear, or joy/happiness). The intensity of the emotional reaction is crucial in determining an individual's action readiness. Action readiness may manifest itself as approach, avoidance, or inaction (Deckers, 2016:339; Keltner & Shiota, 2003:89).

3.5 SITUATIONAL VULNERABILITIES OF INSIDER ESPIONAGE

Within the analytical framework introduced in Section 3.2, the next factor to consider in the context of insider espionage is that of situational vulnerability. The reasoning in this study is that although a trigger may elicit a motivation process which culminates in an individual's willingness to partake in espionage, such acts can only occur if vulnerabilities exist that the individual can exploit. A vulnerability is any weakness in a security system, security procedure, internal control, or security implementation that is susceptible to manipulation (National Institute of Standards and Technology, 2021:n.p.). While there is a paucity of writings on the exploitation of vulnerabilities, there is an abundance of literature that implicitly reflects on specific vulnerabilities by focussing on the security measures that organisations should put into place for the protection of sensitive information. Such literature centres around four themes: 1) vulnerabilities with respect to personnel, 2) vulnerabilities with respect to the physical security system, 3) vulnerabilities with respect to the treatment of information, and 4) vulnerabilities with respect to the ICT setup (European Space Agency, 2020:8, 14, 26 & 33; Mehan, 2016:102; Prunckun, 2019:vii). The aim of the following subsections will be to examine the vulnerabilities that relate to the above-cited four themes.

3.5.1 Vulnerabilities with respect to personnel

Personnel vulnerabilities relate to aspects in an employee's personal background that could, under certain conditions, lead to an insider threat. The vulnerabilities also relate to the system with which such personal aspects should be identified. According to the United States Government (2017:n.p.) vulnerabilities related to an individual's background include:

- Allegiances to unfriendly entities;
- Foreign influence and preferences;
- Personal conduct;
- Financial difficulties;
- Excessive alcohol consumption;
- Drug and substance abuse;
- Psychological conditions;
- Criminal conduct;
- Inappropriate handling of protected information;
- Incompatible outside activities; and
- Inappropriate use of information technology.

A well-functioning personnel security system will have established the measures necessary to identify possible vulnerabilities both before and during an individual's employment by applying the appropriate screening techniques. In order to bring possible points of concern to light, such techniques will typically assess the individual's 1) employment history, 2) educational history, 3) residential history, 4) marital history, 5) personal reference checks, 6) citizenship history, 7) military service history, 8) association history, 9) financial and credit history, and 10) criminal history (Heneman, Judge & Kammeyer-Mueller, 2019:404-405; Prunckun, 2012:110-111).

3.5.2 Vulnerabilities in the physical security system

Physical security is ‘concerned with active, as well as passive measures, designed to prevent unauthorised access to personnel, equipment, installations, materials, and information; and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity’ (Center for Development of Security Excellence, 2015:1-1). Physical security involves the implementation of safeguards through measures such as: site design, protective barriers, security lighting, electronic security systems, access control points, key control and locking system security, and security personnel (Department of the Army, 2010:v). Vulnerabilities in the physical security system may involve any of these elements.

3.5.3 Vulnerabilities in information security

Information security pertains to a system of policies, procedures, and requirements needed for the protection of information which could cause reasonable damage if exposed to unauthorised disclosure (Secretary of the Air Force, 2019:11). Information security includes 1) information classification, 2) use of code names, 3) compartmentalisation, 4) accounting practices, 5) clear desk policies, 6) document storage policies, and 7) document and waste disposal policies (Prunckun, 2019:131). Vulnerabilities in information security systems involve shortcomings related to the above elements.

In governmental organisations and the armed forces, information security systems are clearly defined through well-established standards. In the private sector, information security is addressed through ISO/IEC 27000 standards (Wimmer, 2015:114-115)( ). These standards are, however, largely focussed on information security in the cyber environment and will therefore be addressed in the next subsection. Apart from the ISO/IEC 27000 standards, there are no information security standards in the private sector other than those regulating the handling of classified information when performing work for the government. Systems that are established in the private sector tend to be company-specific and typically based on those used in governmental and military organisations (Wimmer, 2015:114-115).

In governmental and military organisations, the protection of information is based on the classification level that is associated with it. Information ‘could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure requires protection in the interest of national security' (Department of Defense, 2020:40). In that regard, sensitive and protected information is subject to classification as 'Top Secret', 'Secret', or 'Confidential', or 'Only for official use' in some countries (Bundesregierung, 2018:§2; Department of Defense, 2020:40).

3.5.4 Vulnerabilities in Information and Communication Technology (ICT)

Information and communication technologies integrate audio-visual and telephone network (communication) technologies with information network (computer) technologies. Using technical means of telecommunication, they serve the processing, exchange and archiving of information, which is essential for the functioning of organisations. The importance of ICT systems requires special protection with regard to the following:

- **Availability** – ensuring that the information resource is available when it is needed, in the right place, and in the prescribed form;
- **Confidentiality** – ensuring that access to the information resource contained in the system can only be accessed by individuals who are authorised to access it; and
- **Integrity** – ensuring that the original form or state of the information resource can only be modified by individuals who are authorised to modify it (Wąsiński, 2015:72).

Over the past forty years, organisations have increasingly moved towards consolidating and centralising ICT systems as well as the information that they contain. For organisations, this is a way of achieving greater efficiency. However, for an insider spy, this development signifies a greater concentration of information in one place and providing a greater target density and higher target value (Mehan, 2016:75). Most recently, ICT capabilities have improved through the introduction of the cloud and evolution of larger data which has increased the velocity, variety, and volume of available information. Information and communication technologies have also magnified the threat of insider espionage due to the large amounts of retrievable data from a single source with minimal effort (Mehan, 2016:86).

3.5.5 Factor summary

Within the framework depicted above, situational vulnerabilities constitute the third factor of insider espionage. Situational vulnerabilities facilitate acts of espionage by enabling the individual to exploit an existing security system. They may exist with respect to personnel, physical, informational, and ICT security and may take a combination of these vulnerabilities to facilitate insider espionage. A final point to be taken from this discussion is the developments within the field of ICT that have made it possible to purloin vast amounts of documentation to an extent that would have been unimaginable a decade sooner.

3.6 MARKET OPPORTUNITIES OF INSIDER ESPIONAGE

The fourth factor in the framework outlined above is that of the market opportunity. In this context, a market is taken to be a ‘network of dealings in any factor or product’ between customers and suppliers in which ‘the dealings may be regular and organized…[or] spasmodic and unsystematic’ (Cairncross & Sinclair, 1982:20). A market is a system that combines ‘the forces of supply and demand for a particular good or service’ and that consists of customers, suppliers, and mechanisms for effecting transactions (Imber & Toffler, 2000:342). In this sense, espionage is viewed as a market-driven process characterised by the following: 1) the insider spy is the supplier; 2) the handler is the customer; 3) the illicitly provided information constitutes the goods or services; and 4) the benefit that the insider spy expects to gain by providing the information is the incentive to embark on the illicit exchange.

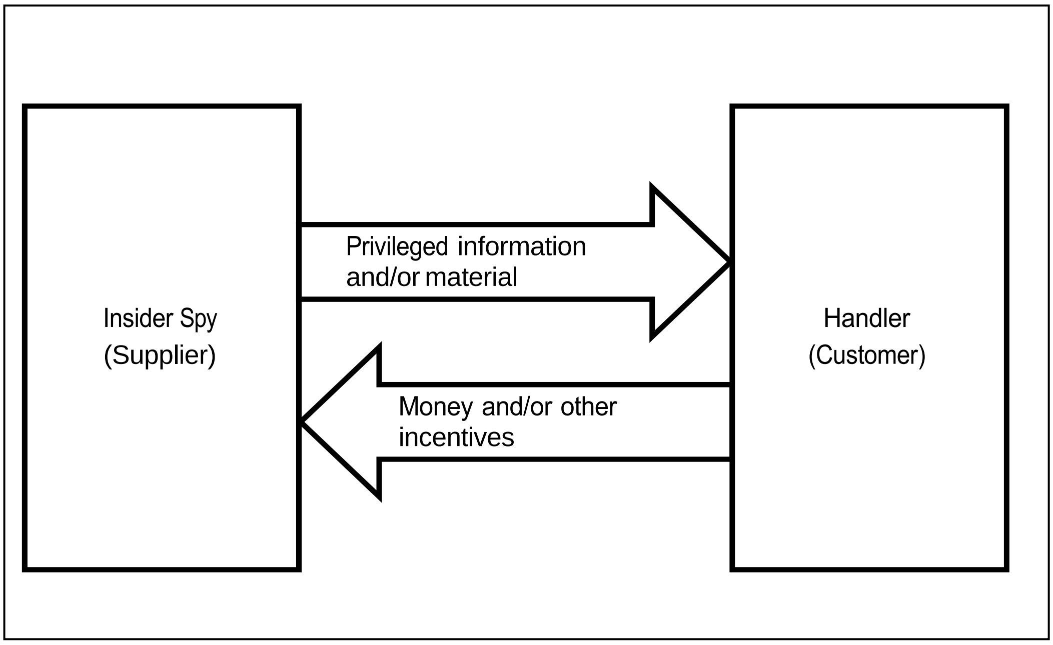


Figure 3.2: Insider espionage exchange relationship

(Source: Developed by the researcher)

Transactions occurring in a market are typically affected with money as a medium of exchange, but may also occur by some form of barter excluding money as an incentive that is provided in exchange for goods or services (Cairncross & Sinclair, 1982:6). In other markets, the transaction between insider spies (suppliers) and handlers (customers) is not based on financial incentives. The incentive for the spy can be non-financial and perhaps even intangible. This is supported by Herbig's (2017) study of 209 cases of insider espionage, according to which, money was the incentive in less than 50% of the cases. In the other cases, the spies were motivated by incentives other than money (Herbig, 2017:45). In view of the pivotal role of incentives in market relationships, the aim of the next subsection is to explore market incentives and how they manifest themselves in cases of insider espionage.

3.6.1 Incentives to commit espionage

An incentive is an external stimulus that attracts an individual if beneficial, or repels the individual if it is detrimental. However, it is not the incentive alone that determines an individual's behaviour. An incentive will only have an effect if it corresponds with an existing motive either by supporting a positive outcome or preventing a negative one (Deckers, 2016:45). Motives relate to an individual's needs, beliefs, values, ideologies and push the individual to reach some desired end-state. Incentives are the counterparts of motives and have a pulling effect because they are expected to offer satisfactory outcomes with respect to an individual's needs, beliefs, values, or ideologies (Deckers, 2016:3; Griggs & Jackson, 2020:178; Maslow, 1970/1987:60-63; Nolen-Hoeksema et al., 2014:347).

To understand how stimuli can act as incentives, it is important to understand the motives with which they correspond (Deckers, 2016:362). According to a study by Herbig (2017:45) most cases of insider espionage centre around six themes: 1) money, 2) disgruntlement, 3) ingratiation, 4) coercion, 5) thrills, and 6) recognition or ego. Based on cases extracted from the Defense Personnel Security Research Center (cf. 2009) and Herbig (cf. 2017), these themes can serve to illustrate the relationship between triggers, motives, and market incentives. Table 3.6 draws on the six themes identified by Herbig (2017:45) but it adds a further distinction between cases surrounding the theme of money as some instances of espionage are prompted by financial need and others by greed. With this distinction, the table offers seven themes. The researcher has identified an insider espionage case for each of these themes and reflected the trigger, motive, and incentive for each one of them. The table indicates what motive each of the insider spies had and what incentive attracted or repelled them. Ultimately, it was as a result of the interplay between the motives and incentives that these individuals were prepared to supply their handlers with secret information. To fully understand the dynamics of the market for privileged information, it is also necessary to explore the demand side of the exchange relationship. This is addressed in the next subsections.

Table 3.6: Triggers, motives, and incentives

Theme	Case	Trigger	Motive (Desired Condition)	Incentive (Attracted by)
Money (financial need)	Davis Henry Barnett	Barnett resigned from the CIA to start a business that failed leaving him with $100,000 in debts (Defense Personnel Security Research Center, 2009:5).	Need: Security (financial)	Money
Money (greed)	James Hall III	Hall was an Army Warrant Officer who, according to his own accounts was not 'short of money' but did not 'want to worry where the next dollar was coming from' (Defense Personnel Security Research Center, 2009:18-19).	Value: Comfortable lifestyle	Money
Disgruntlement	John Douglas Charlton	Charlton was a research specialist with the Lockheed Corporation who was forced to leave under an early retirement program (Defense Personnel Security Research Center, 2009:8-9).	Value: Equality/justice	Satisfaction through revenge
Ingratiation	John Clayton Lonetree	Lonetree was a U.S. Marine Corps non-commissioned officer based at the American Embassy in Moscow. He was unmarried and romantically linked to a Russian woman, who unbeknownst to him was a KGB officer (Defense Personnel Security Research Center, 2009:34-35).	Need: Love and belongingness	Affection
Coercion	Svetlana Tumanova	Tumanova was an Estonian-born naturalised US citizen who was working as a secretary for the US Army. She was being coerced into espionage by intelligence officers with threats against her parents who still lived in Estonia (Defense Personnel Security Research Center, 2009:58).	Need: Safety and security (for loved ones)	Deliverance from the threat levelled by the intelligence officers

Theme	Case	Trigger	Motive (Desired Condition)	Incentive (Attracted by)
Thrills	Jeffery Loring Pickering	Pickering was a non-commissioned officer with the US Marine Corps. He had the reputation of being a thrill seeker, thief and upon his arrest confessed that he had fantasized about espionage. Through his work, he had access to classified documents (Defense Personnel Security Research Center, 2009:44-45).	Need: Thrills and excitement through high arousal threshold	Thrill of providing classified documents to a foreign intelligence agency
Recognition and ego	Stephen Jin- Woo Kim	Kim was a nuclear proliferation specialist and senior intelligence analyst who was detailed to the DoD's Bureau of Verification, Compliance, and Implementation. Kim made the acquaintance with James Rosen, a reporter for Fox News, who interviewed Kim on the situation in North Korea. According to his own account, Kim was flattered by the attention he was receiving from a nationally known reporter (Herbig, 2017:89-91).	Need: Self- esteem	Recognition (e.g. flattery) from a respected or admired individual

(Source: Compiled by the researcher)

3.6.2 The role of policy in creating demand for espionage

The demand for specific types of intelligence is typically driven by policy (Omand, 2014:60). It is incumbent upon policymakers in both public and private sectors to formulate policies and ensure their implementation. Policies are guiding principles that determine the direction and shape of the future. Policies have to do with the 'choice of purposes, molding [national or] organizational identity and character, the continuous definition of what needs to be done, and the mobilisation of resources for the attainment of goals in the face of competition or adverse circumstances' (Christensen, Andrews & Bower, 1978:3). In the public sector, national policies may relate to a variety of issues including foreign relations, security and defence, industrialisation, and commerce (Lipson, 1977:13-14 & 399). In the private sector, corporate policies relate to a range of issues including markets, products, research and development (R&D), staffing, and investment strategies (Fisher, 2015:1).

Amongst the most integral challenges that policymakers face, both in the public and private sectors, is that of incomplete information. To bridge the information gap and to overcome the uncertainties that information gaps cause, policymakers depend on the information provided through a variety of intelligence sources. In the public sector, this information is *inter alia* provided through a system of strategic and national security intelligence (Johnson, 2010:5; Kent, 1966:3-5). In the private sector, it is through corporate intelligence that policymakers bridge information deficits (Fisher, 2015:1). If the collection and dissemination of intelligence violates existing laws, it is referred to as espionage.

The collection of intelligence is a goal-directed activity both in the public and the private sector. The way in which intelligence activities unfold is reflected in what intelligence scholars and practitioners refer to as the intelligence cycle. The intelligence cycle characterises the intelligence process as a sequence procedure arranged in a feedback loop. In its basic form, the intelligence cycle consists of five steps: 1) Planning and Direction, 2) Collection, 3) Processing, 4) Analysis and Production, and 5) Dissemination (Central Intelligence Agency, 2020:26-27; Omand, 2014:59). Planning and direction refer to the control of the complete intelligence effort through its various steps. It is through this step that policymakers define their intelligence requirements in support of their impending decision processes and that handlers subsequently receive the mandate to collect specific information which might include that which is illicitly acquired.

Collection is the process in which the raw information is gathered through one or more of the basic intelligence sources or collection disciplines. Processing involves converting raw information into a format that can be exploited by analysts. Analysis and production is the step in which the processed information is converted into finished intelligence products that can be delivered to policymakers. Dissemination is the provision of the final intelligence products to policymakers who initiated the intelligence cycle (Canadian Security Intelligence Service, 2020:9-10; Central Intelligence Agency 2020:26-27; Omand, 2014:59).

3.6.3 The demand for information

The information that is in demand depends on the prospective recipient. For purposes of analysis, it is therefore beneficial to distinguish between the demand of state actors (governments) and corporate actors. Governmental agencies responsible for protecting their country against espionage and investigating such cases emphasise that '[i]ntelligence agencies are directed by their governments to focus their attention on specific priorities' (Security Service MI5, 2021:n.p.). For the governments of most countries, having access to sensitive information from abroad is of the utmost importance to develop their policies, react to global crises, and to achieve their global political objectives. Diplomats typically gather information that is available in the public domain to inform their governments of current events and longer-term developments, and to promote their own countries' relations with the host country. However, many governments are not satisfied with obtaining open-source information alone. There is also the intention to gain insights that are not accessible to the public. This is where the realm of espionage begins (Bundesamt für Verfassungsschutz, 2021:n.p.).

Countries that gather information through espionage typically target political and governmental organisations including the military, as well as industries and organisations (public and private) that are involved in science and research activities (Security Service MI5, 2021:n.p.; Bundesamt für Verfassungsschutz, 2021:n.p.;

Government of Canada, 2020:n.p.). Espionage activities are not, however, only directed at national entities. Intergovernmental organisations like the United Nations, the African Union, the European Union, and NATO can also be possible sites of espionage activity. In part, this is because 1) commercial, technical, and political information is often more readily available, 2) the employees of such organisations enjoy functional or diplomatic immunities, and 3) the security measures are sometimes not as stringent as in their national counterparts (AIVD, n.d.; Bosco, 2012:n.p.; Bundesministerium des Innern, 2020b:39).

In the private sector, a trade secret is a type of intellectual property from which a company derives a benefit and competitive advantage because the company’s know-how is not publicly known (Herbig, 2017:146). The risk of espionage emanates from two sources: state actors and corporate competitors. When espionage is conducted on behalf of a corporate competitor, it is for the purpose of enabling the competitor to achieve an important advantage vis-à-vis the targeted company. The theft of trade secrets enables competitors to circumvent a variety of costly processes, thus allowing them to offer their products at a considerably lower price. This advantage can eventually lead to the competitor gaining so large a market share that the targeted company is eventually driven out of the market and possibly into bankruptcy (Bayerisches Landesamt für Verfassungsschutz, 2021:n.p.; International Chamber of Commerce - Austria, 2021:n.p.).

3.6.4 Marketable information

The information sought by governmental and corporate customers covers a wide field. The specifics depend on the governmental or corporate objectives. Marketable information can be categorised into three broad spectrums: 1) Political and governmental, 2) military, and 3) industrial and research (Bundesministerium des Inneren, 2020:n.p.; Security Service MI5, 2021:n.p.). Political and government secrets include the status of confidential discussions within the government, matters related to governmental policies and security, planned negotiation positions and strategies, as well as economic developments that have not been publicly communicated. Political and government secrets essentially include all information that can be used by foreign governments to gain an advantage in areas like international relations and intelligence operations (Bundesministerium des Inneren, 2020:n.p.; Security Service MI5, 2021:n.p.).

Military secrets include classified information related to the national defence strategy, theatre strategies and operation plans, as well as troop dispositions, locations, strength, and expected courses of action (Bouchat, 2007:3-4; Department of the Army, 2010:E10; Security Service MI5, 2021:n.p.). This category also includes information about the capabilities of and technologies available to the military. Table 3.7 below list the various forms of defence technologies that are specifically protected under ITAR (National Archives, 2021:n.p.).

Table 3.7: Technologies controlled under ITAR

• Firearms, Close Assault Weapons and Combat Shotguns, Guns and Armament • Ammunition/Ordnance • Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, • Bombs, and Mines • Explosives and Energetic Materials, Propellants, Incendiary Agents, and their Constituents • Surface Vessels of War and Special Naval Equipment • Ground Vehicles • Aircraft and Related Articles • Military Training Equipment and Training • Personal Protective Equipment • Military Electronics • Fire Control, Range Finder, Optical and Guidance and Control Equipment	• Materials and Miscellaneous Articles • Toxicological Agents, Including Chemical Agents, Biological Agents • Associated Equipment • Spacecraft and Related Articles • Nuclear Weapons Related Articles • Classified Articles, Technical Data, and Defence Services Not Otherwise Enumerated • Directed Energy Weapons • Gas Turbine Engines and Associated Equipment • Submersible Vessels and Related Articles • Articles, Technical Data, and Defence Services Not Otherwise Enumerated

(Source: National Archives, 2021:n.p.)

Espionage in the private sector is directed at illicitly acquiring the intellectual property of industrial and research organisations that have not been made available in the public domain (Bundesministerium des Inneren, 2020:n.p.). Sectors that are particularly attractive to foreign governments and corporate competitors include ‘aerospace, biopharmaceutical, biotechnology, chemicals, communications, computers, healthcare, information technology, lasers, optics and electronics, mining and metallurgy, nuclear energy, oil and gas, as well as the environment’ (Government of Canada, 2020:n.p.; Security Service MI5, 2021:n.p.). Table 3.8 lists the most coveted types of industrial research and technology sought after by insider spies. Companies involved in research and development activities in these areas are particularly at risk of becoming targets of insider espionage.

Table 3.8: List of frequently targeted industrial research and technologies

• Aeronautics systems • Armaments • Energetic materials • Chemical and biological systems • Kinetic energy systems • Electronics • Ground systems • Guidance, navigation, and vehicle control	• Information systems • Manufacturing and fabrication • Marine systems • Materials • Nuclear systems • Power systems • Sensors and lasers • Signature control • Space systems

(Source: Nasheri, 2005:63)

Apart from the sought-after industrial research and technologies, governmental, and corporate actors are in pursuit of intellectual property. Table 3.9 lists the different forms of intellectual property that are at risk of becoming the target of espionage attacks. Intellectual property includes trade secrets which may vary and include 'all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes …' (Herbig, 2017:146; United States Congress, 1996:n.p.).

Table 3.9: List of frequently targeted types of intellectual property

• Proprietary formulas and processes • Prototypes and blueprints • Research • Technical components and plans • Confidential documents • Computer access protocols • Passwords • Employee data • Manufacturing plans • Equipment specifications • Vendor information • Customer data • Access control information	• Computer network design software (including source codes) • Phone directories • Hiring/firing strategies and plans • Negotiation strategies • Sales forecasts • Pricing strategies • Corporate strategies • Marketing strategies • Positioning strategies • Budget estimates/expenditures • Investment data

(Source: Federal Bureau of Investigation, 2021:1)

3.6.5 Factor summary

The fourth factor in the analytical framework outlined in Section 3.2 is that of the market opportunity. A market is a system that merges ‘the forces of supply and demand for a particular good or service’ and that includes customers, suppliers, and mechanisms for effecting transactions (Imber & Toffler, 2000:342). Espionage can be understood as a market-driven process in which 1) the insider spy is the supplier, 2) the handler is the customer, 3) the illicitly provided information constitutes the goods or services, and 4) the benefit that the insider spy expects to gain by providing the information is the incentive to embark on the illicit exchange.

Insider spies are the suppliers of illicitly acquired information. The incentive to commit insider espionage depends on the needs, beliefs, values, or ideologies that the spies wish to see fulfilled. Examples are offered in Table 3.6 which suggest that the incentive to satisfy the need for financial security is money; the incentive for the need of self-esteem is recognition; and the incentive for the need of safety that is threatened through blackmail or coercion is deliverance from a threat. These determine the insider spy’s willingness to engage in an exchange with a governmental or corporate customer. On the demand side, marketable information can be divided into three broad categories: 1) political and governmental, 2) military, and 3) industrial and research. Potential customers for this information are typically foreign governments or private corporations (Bundesministerium des Inneren, 2020:n.p.; Security Service MI5, 2021:n.p.).

3.7 FACTORS IN THE DECISION TO COMMIT ESPIONAGE

According to the analytical framework introduced in Section 3.2, the final contributing factor to consider in the context of insider espionage is that of the disinhibiting factors. The reasoning behind this consideration can best be explained with the following narrative. At the outset of a process that eventually leads to insider espionage, there is an event or situation that resonates with an individual’s predispositions (i.e., needs, beliefs, values, ideologies) and therefore acts as a trigger for a motivation process (Deckers, 2016:369; McClelland, 1987:6; Rokeach, 1968:113). The motivation process that follows from this consists of a positive or negative appraisal and emotional response (i.e., anger, sadness, fear, or happiness) which, if powerful enough, leads to the individual’s action readiness

(Deckers, 2016:359 & 369-370; Ortony & Turner, 1990:316; Roseman & Smith, 2001:3). Action readiness means the preparedness to take some course of action that – from the individual's point of view - would be an appropriate response to the trigger. At this point, however, the individual has not yet decided which course of action to take because the options remain undetermined (Deckers, 2016:359).

The selected course of action depends on the options that are open to the individual. In the case of insider espionage, there are two factors that must be present: situational vulnerability and market opportunity. For insider espionage to become viable, it is necessary to bring stolen information into one's possession through existing vulnerabilities in the organisation's security system (i.e., personnel security, physical security, information security, and ICT security) (European Space Agency, 2020:8, 14, 26 & 33; Mehan, 2016:102; Prunckun, 2019:vii). It is also necessary to have access to a customer (governmental or corporate) for the stolen information and a market dynamic that would enable the exchange (Bundesministerium des Inneren, 2020:n.p.; Security Service MI5, 2021:n.p.).

Thus, it is through the interplay of action readiness, exploitable situational vulnerability, and existing market opportunity that the act of espionage becomes viable. However, the viability of espionage does not mean that the individual would necessarily choose the option of insider espionage, which is a crime most individuals are inhibited to commit (Heuer, 2001:n.p.). The focus of this subsection, therefore, is on the factors that may either reduce or prevent the emergence of the inhibitions to break the law. However, to understand how these factors work, it is essential to first clarify the relationship between decisions, judgement, and disinhibiting factors. These points will be addressed in the following subsections.

3.7.1 Decisions, judgment and disinhibiting factors

According to Newell, Lagnado and Shanks (2015:20), a decision is 'a commitment to a course of action' which is often preceded by the decision maker's judgement. The judgements themselves are founded on available information at the decision-making moment regarding assessment of the likelihood of a given event occurring (Eysenck & Brysbaert, 2018:397 & 399; Newell et al., 2015:20).

There are differing views among researchers with respect to the completeness of information with which judgements are made and the extent to which rationality prevails in decision processes. In the field of economics, researchers have developed decision models based on the assumptions that:

- Decision makers strive to maximise their net benefits;
- They are completely informed with respect to all possible options and outcomes of their decision;
- They are fully aware of subtle distinctions among decision options; and
- They are completely rational when making their decisions (Sternberg & Sternberg, 2017:441).

The notion that options are chosen rationally on the premise of complete information is still applied in economic research, and it is used as a normative yardstick against which actual decision behaviour is measured (Newell et al., 2015:21-22). However, Simon's (1972:163) theory of 'bounded rationality' has become an important alternative view in decision studies. This theory suggests that the rationality of a decision process is limited because decisions are typically made on the basis of incomplete information (Simon, 1972:163). This view is echoed by Eysenck and Brysbaert (2018:397) who assert that judgements are formed on the basis of available information which is never complete. Within these constraints, decisions are made so as to achieve the best possible outcome given the information that is available.

Judgement, however, is not only affected by bounded rationality in the sense proposed by Simon (1972:163). It can also be adversely influenced by 1) emotional reactions and affect, 2) personality structure, 3) mental disorders, and 4) substance abuse and addictions (American Psychiatric Association, 2013:20; Deckers, 2016:41-47 & 359; Keltner & Shiota, 2003:89). It is important to recognise the influences on judgement due to the disinhibiting affect they may have. For this reason, these variables will be examined closely in the following subsections.

3.7.2 Emotional reactions and affect

In Section 3.4.2, it was suggested that emotions influence how humans react to events and situations. According to the analysis, it is one's emotional reaction that determines one's action readiness (Deckers, 2016:359; Keltner & Shiota, 2003:89). In the present section, however, it is being suggested that emotions also affect an individual's judgment and with that also the decisions that an individual makes with respect to his or her intended course of action. In the field of cognitive psychology, this notion is supported by a sizable body of literature that relates to basic emotions (see Section 3.4.2), judgment and decision making (Angie, Connelly, Waples & Kligyte, 2011:1395; Eysenck & Brysbaert, 2018:472; Ortony & Turner, 1990:316).

Anger is an emotion that results from events and situations which threaten or thwart an individual's goals by providing outcomes that the individual considers negative (Angie et al., 2011:1395 & 1414). Angry individuals resort to heuristics (i.e., cognitive 'shortcuts') rather than systematic information processing while making their decisions (Tiedens & Linton, 2001:974). Given a choice of alternatives, individuals who are angry are more likely than others to choose risky alternatives (Lerner & Keltner, 2001:154-156). This may ultimately motivate them to 'take some action against the causal agent' that is, in their view, responsible for the obstruction (Angie et al., 2011:1395 & 1414).

Anger has been noted as an essential factor in numerous insider espionage cases. Former U.S. Air Force sergeant John Allen Davies, for instance, was angry at the Air Force for discharging him from active service for reasons of poor performance. According to his own accounts he decided to become a spy 'out of revenge because of the unfair way he was treated while in the Air Force' (Defense Personnel Security Research Center, 2009:11). FBI agent Robert Hanssen was reported as being disgruntled whenever he was not awarded an advancement (Vise, 2002:n.p.). Former Lockheed engineer John Douglas Charlton was extremely disgruntled after having been sent on early retirement under less than favourable conditions (Sneiderman, Slater & Glionna, 1995:n.p.). Polish People's Army Colonel Ryszard Kukliński was, by his own account, enraged by his country's involvement in support of the Soviet Army operation to crush the peaceful Prague Spring movement in Czechoslovakia in August 1968 (Weiser, 2004:48-49). Army Warrant Officer James

Hall resented being financially disadvantaged, and finally decided that he would devise means to enrich himself (Chu, 1996:n.p.).

Happiness is associated with feelings of elation and light-heartedness. Like individuals who are angry, those who feel happy are most likely to use heuristics rather than systematic information processing when making decisions. This may be due to an elevated sense of certainty that is attributable to the circumstances inducing this emotion. It is also this sense of certainty that prompts happy individuals to be more inclined to estimate a higher probability of positive outcomes than negative outcomes. (Tiedens & Linton, 2001:973).

While individuals experiencing anger are likelier to choose risky options, those who are happy tend to be more conservative by granting the safe option preference over the risky one (Chuang & Hung-Ming, 2007:71). Differences in the circumstances may explain the difference in decision outcomes. Those who are angry feel the need for control but seek change which motivates them to accept greater risks, whereas those who are happy will usually strive to maintain the status quo, which is often the safer option (Tiedens & Linton, 2001:973).

There are instances in which joy and happiness have been weaponised by operatives who sought to impair an individual's judgement by inducing some form of pleasure and contentment. This could then be leveraged to instigate the individual's acts of espionage. Operations such as these play on ingratiation and involve enticing the target victim (prospective insider spy) by instilling in him or her the 'desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors' (Wimmer, 2015:9).

An example of such enticement tactics was observed in the case of Leandro Aragoncillo, who was a naturalised US citizen of Philippine origin. Aragoncillo had joined the Marine Corps and was eventually appointed to the White House as a staff assistant to military advisors in the Office of Vice President Gore. During an official state visit of Philippine President Joseph Estrada to the White House, Aragoncillo had the opportunity to meet Estrada and members of his staff. Aragoncillo was later approached by an Estrada associate who asked whether Aragoncillo would be prepared to provide American intelligence that could possibly be useful in saving

Estrada’s presidency. Aragoncillo felt flattered by the request and was happy to oblige. He saw an opportunity to ingratiate himself with high-ranking members of the Philippine government (Defense Personnel Security Research Center, 2009:4).

This leveraging also occurs in the ‘honey-trap’ and ‘Romeo’ operations, in which operatives use romantic or sexual relations to manoeuvre (seduce) insiders into providing classified or otherwise privileged information and commit espionage (Charney & Irvin, 2016:11). Clayton Lonetree offers a case in point. He was a Marine Corps security guard at the US Embassy in Moscow, during which he was embroiled in an amorous relationship with a woman who turned out to be a KGB agent who then persuaded Lonetree to provide her with classified documentation (Defense Personnel Security Research Center, 2009:34).

‘Honey trap’ and ‘Romeo’ operations do not always remain romantic or sexually enticing. They can also become blatantly hostile if the targeted victim begins to regret his or her actions and attempts to become uncooperative. Honey trap and Romeo operations can, therefore, also be the prelude to fear-inducing, coercive and extortive measures.

Fear has been described as a ‘sense of impending evil’ which results from the perception of a threat, uncertainty about the threat, and uncertainty about one’s own ability to cope with the threat (Frijda, 1986:74 & 197). If a situation causes an individual to feel fearful, the individual’s goal will likely be to escape from the perceived impending danger (Angie et al., 2011:1415; Izard, 1993:82 & 85-86). People experiencing fear tend to process information using heuristics (stereotyping) rather than to engage in lengthy systematic or rational information processing (Tiedens & Linton, 2001:979). When people experience fear, they feel the loss of control and are more likely to associate risk with a given action or situation (Lerner & Keltner, 2001:154-156; Tiedens & Linton, 2001:974). In this sort of situation, they are likelier to choose what they perceive to be the safest of their alternatives (Lerner & Keltner, 2001:154-156).

Fear has been a key factor in a variety of insider espionage cases. Both, FBI agent Robert Hanssen and Italian Navy captain Walter Biot faced significant financial difficulties and were reported to have been fearful and unable to make financial ends meet (BBC, 2021; Vise, 2002). In a hostile honeytrap operation, U.S. Army Non-Commissioned Officer Roy Rhodes had or at least was made to believe that he had a one-night stand with a Soviet agent while heavily intoxicated. He was then told that the agent was pregnant and that this would be communicated to Rhodes' wife unless he cooperated with Soviet authorities. For fear of the consequences, Rhodes agreed to commit espionage (Wimmer, 2015:86). John Vassall was a British civil servant who was also entrapped in a KGB hostile honeytrap operation. He was seduced into having sex with multiple male partners while drunk. KGB agents photographed him in the act and subsequently blackmailed him with the threat of publicising the photographs unless he provided them with secret information. Like Rhodes, Vassall agreed to commit espionage for fear of being exposed (Wimmer, 2015:87).

Sadness is an emotion that is associated with emptiness or barrenness and 'the explicit absence of something valued' (Frijda, 2010:199). Of the four emotions discussed in this section, it is the only one which is associated with systematic, thoughtful, and detail-oriented cognitive processing (Tiedens & Linton, 2001:975). Individuals who are sad are far more likely to experience a sense of desperation and engage in acts of resignation because they are likelier than others, who are not experiencing sadness, to expect their situations to have a negative outcome. The sense of hopelessness prompts individuals who are sad to accept the risks associated with less safe options, to retreat from or to avoid the sadness-invoking situation, and thus to find a way out of their misery (Angie et al., 2011:1415; Chuang & Hung-Ming, 2007:71).

The effects of sadness in various cases of insider espionage are evident. One such case is that of William Kampiles who was a watch officer at the CIA Operations Center. It was his aspiration to become a field agent and he was profoundly disappointed to learn that this would not be possible because he lacked the necessary qualifications. This prompted him to resign from the CIA. He did not, however, abandon his reverie. In a carefully planned scheme, the watch officer purloined a Top-Secret technical manual on the KH-11 ('Big Bird') reconnaissance satellite prior to his departure from the CIA, and sold the document to a Soviet intelligence officer in Greece. Upon his return to the United States, he reapplied for a position with the CIA. During the job interview he was hoping to demonstrate his prowess as a field agent and possibly even as a double agent by recounting his actions. However, instead of being hired as a field agent, he was handed over to the FBI and was subsequently arrested and eventually imprisoned for espionage (Defense Personnel Security Research Center, 2009:27).

3.7.3 Personality structure

There is a considerable amount of literature that suggests that personality structure affects the decisions that people make and their subsequent behaviours (Deckers, 2016:41-47). In the 1980s, a new taxonomic model gained momentum in the field of psychology, and has since gained widespread acceptance. This model, known as the five-factor model or the ‘Big Five’, posits that variations between people can be explained on the basis of five personality factors: 1) neuroticism, 2) extraversion, 3) openness, 4) ‘agreeableness’, and 5) conscientiousness (Barrick & Mount, 1991:849; Costa & McCrae, 1985:1; Digman, 1990:417; Gross, 2019:723).

Based on the work of Zuckerman (cf. 1994), Zuckerman, Kuhlman, Joireman, Teta and Kraft (cf. 1993), and Zuckerman, Kuhlman, Thornquist, and Kiers (cf. 1991), Deckers (2016:233) has, like countless other psychologists, adopted the five-factor model in his work. However, Deckers (2016:233) asserts that there is an additional factor which is not addressed in the five-factor model, but which is also linked to differences in behaviour, namely: sensation seeking (Deckers, 2016:233). Regarding insider espionage, this addition is highly relevant because thrill seeking, as one type of sensation seeking, has reportedly been a driving factor in a number of espionage cases (Defense Personnel Security Research Center, 2009:30 & 45; Herbig, 2017:46). Table 3.10 below depicts the ‘Big Five’ personality factors as well as the additional factor of sensation-seeking and provides a description of each.

Table 3.10: Description of the personality dimensions

Personality dimension	Description of the personality dimension
Neuroticism	At the high end, neuroticism correlates with the tendency to be emotional, anxious, and quickly aroused; at the low-end neuroticism correlates with a calm, stable, and contented disposition (Deckers, 2016:245, Hewstone, Finchham & Foster, 2005:300).

Personality dimension	Description of the personality dimension
Extraversion	Extraversion describes the tendency of the individual to seek, and interact with others. Introversion describes the tendency to be quiet and shy displaying retiring, sober, and reserved behaviours (Deckers, 2016:233; Hewstone et al., 2005:300).
Openness	Individuals with high openness tend to prefer variety, diversity, and independence. Individuals with low openness tend to prefer routine and conformity (Hewstone et al., 2005:302).
'Agreeableness'	High levels of 'agreeableness' suggest that the individual tends to be trusting, compliant, soft hearted, and helpful. In contrast, those whose 'agreeableness' is low, tend to be ruthless, suspicious, and uncooperative (Hewstone et al., 2005:302).
Conscientiousness	Individuals with high levels of conscientiousness tend to be competent, orderly, and dutiful. They are achievement oriented, self-disciplined, and deliberate in their actions. Individuals who have low levels of conscientiousness tend to lack these characteristics (Hewstone et al., 2005:302).
Sensation Seeking	Sensation-seeking is associated with ''a lack of planning and the tendency to act impulsively without thinking' (Zuckerman et al., 1991:758) and the tendency to seek 'varied, novel, complex, and intense sensations and experiences, and the willingness to take physical, social, legal, and financial risks for the sake of such experience' (Zuckerman, 1994:27).

(Source: Compiled by the researcher)

Eysenck (1977:49-52 & 57-60) hypothesised that individuals who are highly neurotic and extraverted were more prone to be criminally predisposed than those who are not, particularly when they also show signs of psychoticism. Eysenck (1977:49-52) further reasoned that neurotic individuals tended to be more anxious than others, and also responded more intensely to aversive stimuli. In his view, extraverted individuals are generally under-stimulated, and require intense external stimulation (excitement) to compensate for the lack thereof. Eysenck (1977:49-52 & 57-60) contends further that both neuroticism and extraversion make it unlikely for normal processes of socialisation to succeed, and that criminal behaviour would consequently become more probable in such instances (Putwain & Sammons, 2003:38-39).

While subsequent empirical studies demonstrated that neuroticism and psychoticism significantly correlate with criminal behaviour, extraversion did not. The results regarding extroversion have been inconsistent. In some instances, even suggesting that offenders scored lower on extraversion than non-offenders (Hollin, 1992:75; Putwain & Sammons, 2003:39-40).

Openness is a personality factor associated with a preference for variety, diversity, and independence. Lower assessments of openness are linked with closed mindedness and ambiguity intolerance (Gøtzsche-Astrup, 2019:103). Individuals with low openness levels tend to prefer routine and conformity (Hewstone et al., 2005:302). In a political context, lower levels of openness are associated with a social dominance orientation and authoritarianism. These characteristics serve as predictors for extreme political behaviour, including political violence and aggression (Gøtzsche-Astrup, 2019:103).

Individuals who are highly agreeable tend to be trusting, compliant, soft-hearted, and helpful, whereas those who are further down in the ‘agreeableness’ scale were prone to ruthlessness, distrust, and obstructiveness (Hewstone et al., 2005:302). According to Webster, (2018:131) and Brandstätter and Opp (2014:518), ‘agreeableness’ is negatively correlated with hostility (Brandstätter & Opp, 2014:518; Webster, 2018:131).

Conscientiousness relates to competence, orderliness, and dutifulness. Individuals who are achievement oriented, self-disciplined, and deliberate in their actions, tended to score highly in the conscientiousness scale. Individuals who have low levels of conscientiousness tend to lack these characteristics (Hewstone et al., 2005:302). According to Brandstätter and Opp (2014:518), conscientiousness does not appear to be a major correlate of political hostility.

Sensation-seeking is associated with ‘a lack of planning and the tendency to act impulsively without thinking’ (Zuckerman et al., 1991:758); as well as the tendency to seek ‘varied, novel, complex, and intense sensations and experiences, and the willingness to take physical, social, legal, and financial risks for the sake of such experience’ (Zuckerman, 1994:27). Craig and Piquero (2017:1376-1377) distinguish between unsocialised sensation seeking (USS) and socialised sensation seeking (SSS). In their study of differences between both socialised and unsocialised sensation seeking and crime, the researchers found that both USS and

SSS are positively correlated with low self-control. However, while USS is a positive predictor of the intention to offend, SSS is not (Craig & Piquero, 2017:1376-1377).

3.7.4 Mental disorders

Mental disorder is ‘a syndrome characterised by a clinically significant disturbance in an individual's cognition, emotion regulation, or behaviour that reflects a dysfunction in the psychological, biological, or developmental processes underlying mental functioning’ (American Psychiatric Association, 2013:20). In addition, mental disorders include a very broad range of syndromes, most of which are less directed to the current subject. There are, however, four categories of mental disorder that have been reported as contributing factors in criminal behaviour or, more specifically, in espionage: bipolar disorders (Herbig, 2008:46, 52, 55 & 70); personality disorders (Shechter & Lang, 2011:2); psychopathic disorders (Hicks & Drislane, 2018:299); and substance-related and addictive disorders (Heuer, 1994:iii).

According to a study by Herbig (2008), four of eleven individuals guilty of espionage were found to have had ‘serious mental and emotional problems’ (Herbig, 2008:64). One offender was described as mentally ‘brittle, immature and impulsive’. The diagnosis, however, does not appear to have been made publicly available. In the other three cases, the offenders were diagnosed with a bipolar disorder (Defense Personnel Security Research Center, 2009:3; Herbig, 2008:46, 52 & 55). While a sample of eleven cases is too small to support general conclusions, the number of bipolar cases within this sample is noteworthy and suggests further consideration of this diagnosis in the context of espionage (Herbig, 2008:70).

Individuals affected by a bipolar disorder (Bipolar I) experience both, manic and depressive episodes. The manic episode is a phase of ‘abnormally and persistently elevated, expansive, or irritable mood and abnormally and persistently increased goal directed activity or energy, lasting at least one week and present most of the day, nearly every day’ (American Psychiatric Association, 2013:123-124). Such episodes are linked to a noticeable change in behaviour marked by three or more of the following: ‘… inflated self-esteem or grandiosity, … decreased need for sleep, … more talkative than usual or pressure to keep talking, … flight of ideas or subjective experience that thoughts are racing, …distractibility, … increase in goal-directed activity, and excessive involvement in activities that have a high potential for painful consequences' (American Psychiatric Association, 2013:124).

During major depressive episodes, individuals suffering from a bipolar I disorder experience a 'depressed mood most of the day, nearly every day, markedly diminished interest or pleasure in all, or almost all, activities most of the day, nearly every day, significant weight loss when not dieting or weight gain or decrease or increase in appetite nearly every day, insomnia or hyper insomnia nearly every day, psychomotor agitation or retardation nearly every day, fatigue or loss of energy nearly every day, feelings of worthlessness or excessive or inappropriate guilt diminished ability to think or concentrate, or indecisiveness, nearly every day, and recurring thoughts of death, recurrent suicidal ideations without a specific plan, or a suicide attempt or a specific plan for committing suicide' (American Psychiatric Association, 2013:124).

A personality disorder is defined as an 'enduring pattern of inner experience and behaviour that deviates markedly from the expectations of the individual's culture, is pervasive and inflexible, and has an onset in adolescence or early adulthood, is stable over time, it leads to distress or impairment' (American Psychiatric Association, 2013:645). According to a study by Shechter and Lang (cf. 2011), certain personality disorders are linked to an elevated 'likelihood of unreliable behaviour, poor judgment, and compromised motivation' that can pose a risk with regard to the handling of classified information and sensitive materials (Shechter & Lang, 2011:2). The latter authors found that three Cluster B personality disorders are associated with the highest level of security risk, which are: antisocial personality disorders, malignant narcissism, and borderline personality disorders (Shechter & Lang, 2011:vii). Table 3.11 lists the diagnostic criteria for each of these disorders. These criteria offer an important insight into the types of observable behaviour that may suggest the presence of the respective disorder. This is most valuable with respect to the identification of factors that could disinhibit decision processes when all other factors in the framework advanced by the researcher favour acts of espionage.

Table 3.11: Diagnostic criteria for antisocial, narcissistic and borderline personality disorders

Antisocial personality disorder occurring since age 15, indicated by three or more of the following:

1. 'Failure to conform to social norms with respect to lawful behaviours, as indicated by repeatedly performing acts that are grounds for arrest.
2. Deceitfulness, as indicated by repeatedly lying, use of aliases, or conning others for personal profit or pleasure.
3. Impulsivity or failure to plan ahead.
4. Irritability and aggressiveness, as indicated by repeated physical fights or assaults.
5. Reckless disregard for safety of self or others.
6. Consistent irresponsibility, as indicated by repeated failure to sustain consistent work behaviour or honour financial obligations.
7. Lack of remorse as indicated by being indifferent to or rationalizing having hurt, mistreated, or stolen from another' (American Psychiatric Association, 2013:659).

Narcissistic personality disorder indicated by five or more of the following:

1. 'Has a grandiose sense of self-importance (e.g. Exaggerates achievements and talents, expects to be recognized as superior without commensurate achievements).
2. Is preoccupied with fantasies of unlimited success, power, brilliance, beauty, or ideal love.
3. Believes that he or she is 'special' and unique and can only be understood by, or should associate with, other special or high-status people (or institutions).
4. Requires excessive admiration.
5. Has a sense of entitlement (i.e. unreasonable expectations of especially favourable treatment or automatic compliance with his or her expectations).
6. Is interpersonally exploitative (i.e. takes advantage of others to achieve his or her own ends).
7. Lacks empathy is unwilling to recognize or identify with the feelings and needs of others.
8. Is often envious of others and believes that others are envious of him or her.
9. Shows arrogant, haughty behaviours or attitudes' (American Psychiatric Association, 2013:669-670).

Borderline personality disorder indicated by five or more of the following:

1. Frantic efforts to avoid real or imagined abandonment.
2. A pattern of unstable and intense interpersonal relationships characterized by alternating between extremes of idealization and devaluation.
3. Identity disturbance: markedly and persistently unstable self-image or sense of self.
4. Impulsivity in at least two areas that are potentially self-damaging (e.g. spending, sex, substance abuse, reckless driving, binge eating).
5. Recurrent suicidal behaviour, gestures, or threats, or self-mutilating behaviour.
6. Affective instability due to a marked reactivity of mood (e.g. intense episodic dysphoria, irritability, for anxiety usually lasting a few hours and only rarely more than a few days).
7. Chronic feelings of emptiness.
8. Inappropriate, intense anger or difficulty controlling anger (e.g. frequent displays of temper, constant anger, recurrent physical fights).
9. Transient, stress related paranoid ideations or severe dissociative symptoms' (American Psychiatric Association, 2013:663).

(Source: American Psychiatric Association, 2013:659, 663 & 670)

Psychopathy is a personality disorder ‘characterised by callous affect, interpersonal ‘exploitiveness’, an impulsive and irresponsible lifestyle, as well as a pattern of early, chronic, and versatile antisocial tendencies’ (Garofalo, Neumann & Velotti, 2021:12641). It is regarded as a developmental disorder associated with core affective traits, such as low empathy, guilt, and remorse, and with antisocial and aggressive behaviours’ as well as with dispositional contempt (Marsh, 2013:1; Schriber, Chung, Sorensen & Robins, 2017:293). In its extreme form, psychopathy affects 1–2% of the general population. Among offenders, psychopathy affects as many as 50% of the population (Marsh, 2013:2).

Table 3.12 lists the diagnostic criteria for psychopathy according to the Revised Psychopathy Checklist. Hare, Neumann and Mokros (2018:42), point out that this checklist is frequently used to assess psychopathic disorders among defendants in court procedures. Based on this checklist, data can either be collected through semi-structured interviews or through the use of ‘high quality collateral and file information alone’. Each of the items in the checklist are marked in an ordinal scale of 0, 1, and 2. Subjects who score 30 or higher would, according to Hare et al. (2018:42), be considered psychopaths.

Table 3.12: Psychopathy checklist – revised (PCL-R)

Factor 1: Interpersonal	**Factor 2: Lifestyle**
• Glibness/superficial charm • Grandiose sense of self worth • Pathological lying • Conning/manipulative	• Need for stimulation • Parasitic lifestyle • No realistic, long-term goals • Impulsivity • Irresponsibility
Affective	**Antisocial Behaviours**
• Lack of remorse of guilt • Shallow affect • Callous/lack of empathy • Failure to accept responsibility	• Poor behavioural controls • Early behavioural problems • Juvenile delinquency • Revoke conditional release • Criminal versatility

(Source: Hare et al., 2018:43)

3.7.5 Substance abuse and addiction

According to the Diagnostic and Statistical Manual of Mental Disorders (DSM-V), the category of substance-related and addictive disorders encompasses a variety of substances (i.e. alcohol, caffeine, cannabis, hallucinogens, inhalants, opioids, sedatives, stimulants, and tobacco) as well as gambling (American Psychiatric Association, 2013:482 & 585). Clearly, not all these disorders pose a security risk. Security concerns typically relate to substance-related and addictive disorders that may diminish inhibitions and self-control, facilitate reckless behaviour, reduce reliability, and/or cause significant financial difficulties that motivate the individual to raise money through illegal means. The markers in this regard include the abuse of legal drugs, the use of illegal drugs, alcohol dependence or abuse, and gambling (Herbig, 2008:41).

According to a study involving 173 individuals involved in insider espionage between 1947 and 2007, 40 (23%) had a history of legal drug abuse or illegal drug use. An equal number had a history of alcohol abuse and/or addiction, and 13 (7.5%) had a gambling disorder (Herbig, 2008:40-41). It is not certain whether the use or abuse of drugs has been a major contributing factor or merely a coincidental factor. Reilly and Joyal (1993) undertook a study with eighteen individuals (ten of whom were regular users of drugs and eight were experimental users), and found that, '[i]n no case did an individual indicate that drugs or the need for drugs drove him to the act of espionage, nor did any commit espionage to support their habit' (Reilly & Joyal, 1993 quoted in Heuer, 1994:2; see also Bosshardt, 2000:37). In a 2009 study involving 141 cases of espionage, however, there was at least one case in which an individual convicted of espionage was motivated 'by the need for money with which he and … [his co- conspirator] could purchase drugs (Defense Personnel Security Research Center, 2009:6).

Regarding the effects of alcohol, the situation may be more predictable. The regular consumption of moderate to high amounts of alcohol is associated with impaired concentration and increased self-confidence; as well as an impairment of an individual's judgement and ability for abstract thought (Schug & Fradella, 2015:150). This may cause an individual to be vulnerable to impulsive behaviour and poor decision-making.

Gambling disorders are characterised by 'persistent and recurrent problematic gambling behaviour leading to clinically significant impairment or distress' (American Psychiatric Association, 2013:585). In order to reach their optimal sense of thrill, people with gambling disorders commonly need to increase the wager amounts. Gambling disorders are also associated with unsuccessful attempts to reduce the amount of gambling, lying to conceal the gambling activities, risking the loss of, or actually neglecting an important bond, employment, or an opportunity in education or even a career (American Psychiatric Association, 2013:585).

3.7.6 Factor summary

Circumstances that render acts of insider espionage viable encompass: the individual's action readiness, the opportunity to illicitly acquire information due to situational vulnerabilities, and the existence of a market for the illicitly acquired information (Herbig, 2017:A4; Heuer, 2001:n.p.). Despite its viability, however, very few people decide to commit insider espionage. What distinguishes those who transgress from the vast majority of those who do not, is that the inhibitions of those who break the law are in some way compromised (Heuer, 2001:n.p.). Inhibitions affect judgment and decision making. They can be neutralised or prevented from emerging through four disinhibiting factors: emotional reactions (affect), personality structures, mental disorders, and substance abuse and addictions (Herbig, 2017:45; Heuer, 2001:n.p.; Prunckun, 2019:vii; Siegel, 2017:103).

Emotional reactions (i.e., anger, sadness, fear, happiness) not only influence action readiness. They also influence judgment and could all be associated with acts of insider espionage (BBC, 2021:n.p.; Defense Personnel Security Research Center, 2009:4, 11 & 27; Vise, 2002:n.p.; Wimmer, 2015:9). Personality characteristics (i.e. neuroticism, openness, extraversion, 'agreeableness', conscientiousness, and sensation seeking) define the most important aspects of personality structure (Barrick & Mount, 1991:849; Costa & McCrae, 1985:1; Deckers, 2016:233; Digman, 1990:417; Gross, 2019:723). Some of these characteristics, more than others, may facilitate the vulnerability of an individual to engage in criminal behaviour. There does not appear to be a correlation between extraversion and criminal behaviour. Neuroticism and psychoticism, however, are significant and positive correlates of such behaviour (Putwain & Sammons, 2003:38-40).

Political violence and aggression have been linked to decreased openness (Gøtzsche-Astrup, 2019:103). Correspondingly, low levels of 'agreeableness' are linked to ruthlessness, suspiciousness, and generally uncooperative behaviour

(Hewstone et al., 2005:302). Not all mental disorders are associated with criminal behaviour or specifically with espionage. However, certain disorders have been identified as markers, including: bipolar, personality, psychopathic, and substance-related and addictive disorders (Herbig, 2008:46, 52, 55 & 70; Shechter & Lang, 2011:2; Hicks & Drislane, 2018:299; Heuer, 1994:iii). In the context of the present study, all of these factors are predictors and any of them may have a disinhibiting effect which could raise the likelihood of a decision favouring espionage.

3.8 CHAPTER SUMMARY

Throughout the discussions from Sections 3.3 through 3.7, the researcher endeavoured to answer two questions:

> **Question 1**: What are the independent variables that are predictors of insider espionage (dependent variable) in the government and private sectors?
> **Question 2**: What are the relationships between the variables of insider espionage in the government and private sectors?

Using the five factors (triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors) that were depicted in Figure 3.1 as a reference point, the researcher systematically explored the independent variables associated with each of these factors. Based on a systematic multidisciplinary analysis, the researcher has identified the key variables associated with each of the factors reflected in Figure 3.3 below, and provided the basis for the theory and ultimately the conceptual framework of insider espionage in Chapter 4.

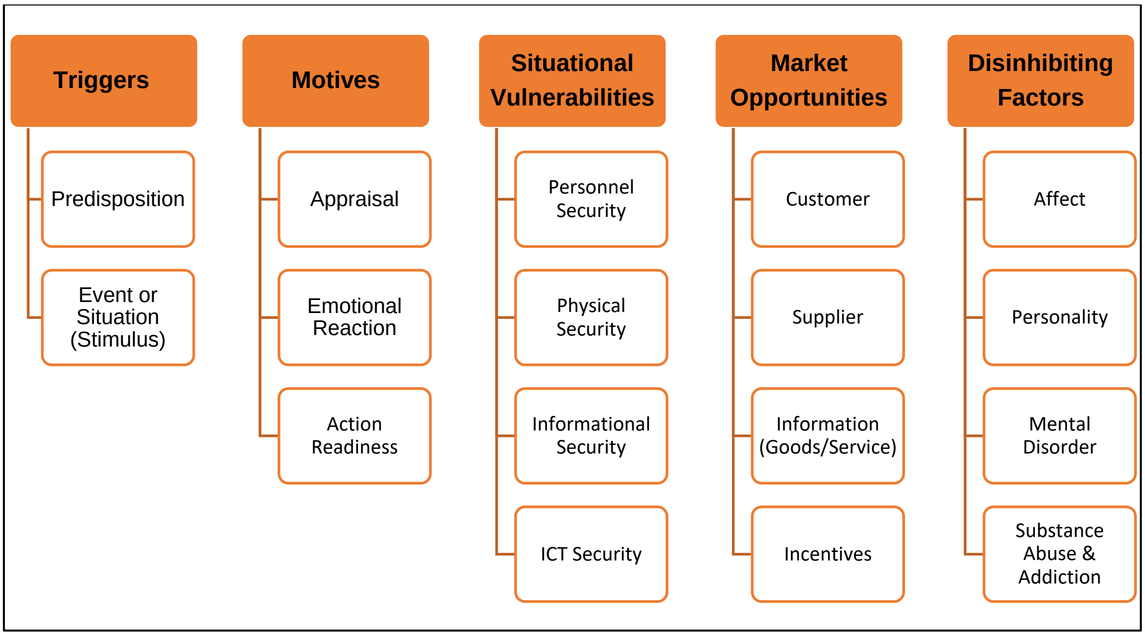


Figure 3.3: Variables of insider espionage

(Source: Developed by the researcher)

According to Jaccard and Jacoby (2010:28), a theory is ‘a set of statements about the relationship(s) between two or more concepts or constructs’. It was through the analyses conducted in Sections 3.3 to 3.7 that the following concepts and their relationships emerged with respect to insider espionage.

The notion that insider espionage is always preceded by a trigger is not new. Heuer (2001) has outlined this in his approach. However, what has remained unclear until now in the context of insider espionage is the reason for the same event or situation being met with indifference by some individuals, while triggering a motivation process in others. Accordingly, the previously absent concept of predisposition (i.e. needs, beliefs, values, ideologies) represents the missing link. It is because of the individual’s predisposition that an event or situation may, or may not act as a trigger: An event or situation becomes a trigger only in the event that it resonates with an individual’s predispositions.

The motivational approaches introduced in Section 1.3.8 provide an overview of motives that have played a role in specific cases of insider espionage. Among these approaches, there is agreement that money - driven either by greed or financial need - has been the incentive that prompted numerous individuals to become spies. However, what these approaches do not explain is why some individuals can be seduced into committing insider espionage for financial gain while others, who are faced with the same circumstances are not at all tempted to do so. What has been absent from the discussion on the motive of insider espionage to date is an explanation why an incentive may become a motive for some but not for others.

By introducing the concepts of appraisal, emotional reaction, and action readiness to the discussion, the researcher has provided an explanation for the individual differences. In this regard, a trigger will lead to an individual's action readiness if, according to the individual's appraisal, the event or situation calls for attention and elicits an emotional reaction that is strong enough to motivate the individual to act. Action readiness, however, is merely the preparedness to act. It is unspecific with respect to the action the individual will choose to take. The choice of action depends on the options that are available to the individual. In the context of insider espionage, these options result from existing situational vulnerabilities in the organisation and market opportunities with respect to the information that the insider spy can provide.

Existing approaches to insider espionage have anecdotally addressed situational vulnerabilities, but have not provided a systematic view on the factor. By drawing on literature in the field of security, the researcher closed the gap by identifying four types of situational vulnerability that facilitate insider espionage: personnel security, physical security, informational security, and ICT security. It is typically some combination of these vulnerabilities that enable the spy to steal his or her organisation's secrets.

The notion that insider espionage depends on the existence of market opportunities, and that the interaction between an insider spy and a handler is based on a market driven exchange, is a further novelty emerging from the researcher's approach. As in any market, the exchange depends on the existence of a supplier, a customer, the goods or services provided by the supplier, and the incentives offered by the customer. In the case of insider espionage, the supplier is the insider spy, the customer is the handler, the goods or services relate to the information that the spy can provide, and the incentives are the tangibles and/ or intangibles that the insider spy receives in exchange. In economic terms, a market interaction will only occur if all four variables are present, and this equally applies to the interaction between an insider spy and his or her handler.

Existing approaches to insider espionage anecdotally address a range of disinhibiting factors that have been involved in specific cases, but do not offer a systematic view of the variables that may affect the individual's decision to become an insider spy. Through his analysis of literature in psychology and psychiatry, the researcher found that the inhibitions that individuals have with respect to breaking the law, are compromised by one or more disinhibiting factors and that these factors fall into four categories (i.e., emotion/affect, personality, mental disorder, and substance abuse/addiction). By performing this systematic analysis, the researcher has further contributed meaningfully to the existing body of literature in the field of insider espionage.

The analyses performed by the researcher in this chapter have aimed at refining the concepts related to insider espionage and clarifying the relationships between these concepts. Such an orientation enabled the researcher to lay the foundation necessary to address the third objective of this research project, which is to construct an interdisciplinary conceptual framework of insider espionage. This is the core subject of the next chapter (Chapter 4).

CHAPTER 4: DEVELOPMENT OF A CONCEPTUAL FRAMEWORK OF INSIDER ESPIONAGE

4.1 INTRODUCTION

The focus of the previous chapter was mainly on responding to research questions 1 and 2 as articulated in Section 1.5 of Chapter 1. It was through the discussion in the preceding chapter (Chapter 3) that the researcher has identified the variables that act as predictors of insider espionage, as well as the relationships between these predictors. Meanwhile, the primary focus of the current chapter (Chapter 4) is on the development of an interdisciplinary conceptual framework of insider espionage in response to the following research question 3 (as articulated in Section 1.5 of Chapter 1):

> **Question 3:** How can the variables of insider espionage and the relationships between them be represented in an interdisciplinary conceptual framework that can serve to predict risks of insider espionage?

Providing an answer to this question is an essential step in this study because it will lay the foundation necessary to address the final research question which will involve the application and validation of the conceptual framework.

4.2 CONCEPTUAL FRAMEWORK OF INSIDER ESPIONAGE

Conceptual frameworks are used to represent theories. They can be presented in a symbolic, postulational, or formal style (Shoemaker, Tankard & Lasorsa, 2003:112). The following function represents the key factors and their interrelatedness as elaborated in the previous chapter in the context of insider espionage:

$$E = f(T, M, V, O, D)$$

where,

E = Insider espionage; T = Trigger; M = Motive; V = Situational vulnerability; O = Market opportunity; and D = Disinhibiting factor.

According to this equation, insider espionage is a function of triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors. In the researcher’s view, this form of representation has merit because it suggests that if any of the independent variables are absent, insider espionage would not occur. This is consistent with the proposition in the researcher's theory that all five factors must be present for insider espionage to occur. This form of representation, however, only characterises the relationship between the independent variables and the dependent variable, but does not characterise the relationships between the independent variables.

The researcher is, therefore, in support of the conceptual framework represented in Figure 4.1 below, which is based on the analysis in Chapter 3 and displays the relationship between all the factors. The researcher regards this figure as being more consistent with his theory. Therefore, the researcher asserts that Figure 4.1 depicts insider espionage as preceded by a trigger that elicits a motivation process culminating in the generation of a motive. The situational vulnerabilities and market opportunities are independent variables, which are cognitively processed together with the motive. In concert, these factors make the act of espionage viable, but not necessarily desirable. If, however, the individual's judgement is adversely affected by disinhibiting factors, the act of espionage is more likely to become desirable. Moreover, if the act of insider espionage leads to satisfactory outcomes for the individual, these outcomes may themselves become triggers that initiate a new cycle of espionage activity. These relationships are further elaborated in the following subsections.

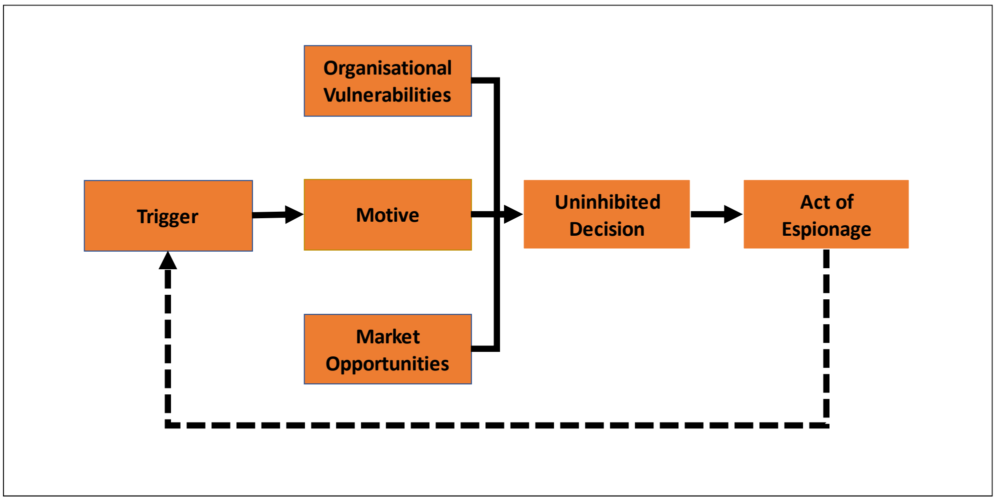


Figure 4.1: High-level conceptual framework of insider espionage

(Source: Developed by the researcher)

4.2.1 Trigger

Acts of espionage are always preceded by a trigger. Triggers can include states of crises, exceptional positive and negative life events, negative organisational incentives, and adverse work conditions. However, more commonplace events or situations like financial problems, professional setbacks, unfair treatment by an employer or supervisor may also be triggers. Essentially, any stimulus can become a trigger if it elicits a reaction, and any event or situation can become a stimulus. This can include the act of espionage itself which may, if successful, prompt the insider spy to repeat the offense.

It is important to realise, however, that events and situations do not have the same effect on everyone, and not every event or situation becomes a trigger. For an event or situation to become a trigger, it must in some way resonate with a person’s predispositions, (i.e., needs, beliefs, values, or ideology). It is through the interplay between an event or situation and an individual’s predisposition that the event or situation could become a trigger. If an event or situation leaves an individual unaffected, it will not become a trigger. However, if the event or situation does in some way resonate with the person’s predispositions, it will act as a trigger and thus initiate a motivation process.

4.2.2 Motives

Motives are the products of motivation processes. Motivation processes, once activated, consist of an appraisal by the individual as to the positive or negative impact of the trigger; an emotional reaction subjectively proportionate with the appraisal of the trigger; and a degree of action-readiness based on the intensity of the emotional reaction. Individuals appraise triggers on the basis of the agreeability, expected effort, validity, attentional activity, and responsibility and control that they associate with the event or situation. Positive appraisals elicit positive emotional reactions, and negative appraisals correspondingly elicit negative emotional reactions.

Emotion is a functional reaction to an event or situation that facilitates a fitness-enhancing, environment-shaping response. There are many different emotions, which are basically clustered into four categories, namely: anger, sadness, fear, and happiness. It is the intensity of an emotion that determines whether or not an individual is prepared to act.

Action readiness is a state of preparedness to engage in some adaptive action that is prompted by an emotion. It is not, however, an action in and of itself. Action readiness may prevail without becoming manifest through action until the time or occasion is there for the action readiness to manifest itself in situation-adapted actions. Depending on the circumstances, such readiness may persist indefinitely. For action readiness to become manifest, individuals must undergo a decision process in which they consider the options available to them. For someone to commit espionage the act does not only depend on the individual’s willingness to act. Independent of one’s action readiness, acts of espionage also depend on the presence of situational vulnerabilities that the insider spy can exploit and on market opportunities which enable the insider spy to acquire the incentives the spy desires in exchange for the information he or she is able and willing to provide.

4.2.3 Situational vulnerabilities

A situational vulnerability is any weakness in a security system, security procedure, internal control, or security implementation that can be exploited by an insider spy. Situational vulnerabilities that enable espionage consist of any combination of factors involving personnel vulnerabilities, vulnerabilities of the physical security system, vulnerabilities concerning the handling of information, and ICT-related vulnerabilities.

4.2.4 Market opportunities

For an opportunity with respect to espionage to exist, it is not just necessary to be able to bring the information into one’s possession, but also to have a market for the information. Espionage is a market-driven process in which the insider spy is the supplier, the handler is the customer, the illicitly provided information constitutes the goods or services, and the benefit that the insider spy expects to gain by providing the information is the incentive to embark on the illicit exchange. Insider spies become involved in espionage because they are attracted to certain incentives. These incentives can be related to any of the individual’s predispositions (i.e. needs, beliefs, values, ideologies).

4.2.5 Disinhibiting factors

Decision processes are motivated by an individual’s action readiness. The decisions individuals make are based on the options of which the individual is aware and the judgements the individual makes with respect to those options. Judgements are assessments of the likelihood of a given event occurring which is based on the available information for decision making. Such judgements may be adversely influenced by any combination of the following:

- Affect (i.e. intense emotional reactions involving anger, sadness, fear, or happiness);
- Personality structure (i.e. high neuroticism, high sensation seeking, low openness, low ‘agreeableness’, low conscientiousness);
- Mental disorders (i.e. antisocial personality disorder, bipolar disorder, malignant narcissism, borderline personality disorder, psychopathic disorders); and
- Substance abuse and addictions (i.e. abuse of legal drugs, gambling, the use of illegal drugs, and alcohol dependence or abuse).

4.2.6 Act of insider espionage

The aforementioned factors are individually necessary and jointly sufficient to predict the risk of insider espionage. The more pronounced each of these factors are, the greater the risk becomes that an individual would be prone to commit insider espionage. The greatest risks of insider espionage exist when individuals are faced with events or situations that significantly affect them in terms of their predispositions; when they appraise the events or situations (triggers) to be extremely negative or positive, consequently have an extreme emotional reaction, and thus become determined to act; when their organisation is highly vulnerable to espionage due to lax or non-existent security; when the information they can illicitly provide is in high demand; and when their inhibitions to commit espionage are significantly compromised. Conversely, if any one of these factors are absent, espionage is highly unlikely to occur.

4.2.7 Espionage as a trigger

Acts of espionage may themselves become triggers if successful in providing the individual with the desired outcomes for example the financial benefit or the revenge that the individual seeks against his or her employer. If, as an event, the act positively resonates with any of the individual’s predispositions and is not outweighed by other considerations (e.g. scruples or fear of detection), it is likely to trigger a new cycle of activity that culminates in a new act of espionage.

4.3 CHAPTER SUMMARY

In this chapter, it has been the researcher’s aim to develop an interdisciplinary conceptual framework that builds on existing literature and systematically addresses each of the concepts and their relationships with respect to acts of insider espionage. According to this conceptual framework, there are five factors preceding such acts: triggers; motives; situational vulnerabilities; market opportunities; and disinhibiting factors. The motivation process involves an appraisal of the trigger and an emotional reaction to the trigger. If the emotional reaction is strong enough, it will prompt the individual’s action readiness. However, action-readiness does not imply that the individual will necessarily engage in espionage. It only means that the individual is prepared to choose a course of action that – in the individual’s view - is a suitable response to the trigger.

Options to commit espionage are created by situational vulnerabilities in the organisation that can be exploited by the individual and by market opportunities which enable a transaction in which the secret information can be exchanged for money or some other incentive. However, even if options to commit espionage exist, the individual’s choice of committing such an act depends on whether or not he/ she is uninhibited with respect to committing espionage. Only if the individual is ready to act and has the option to commit espionage and is unincumbered by inhibitions will he or she commit the act. Since the purpose of this conceptual framework is to explain acts of insider espionage, it lays an important foundation for the analysis of actual cases which will follow in Chapter 5.

CHAPTER 5: CASE STUDY ANALYSIS

5.1 INTRODUCTION

Whereas the preceding chapter (Chapter 4) focussed on the development of a conceptual framework of insider espionage in response to Question 3 (see Section 4.1), the current chapter delves entirely into case study analysis in response to the fourth research question of this study:

> **Question 4:** How can this interdisciplinary conceptual framework be applied to specific cases of insider espionage to identify the presence of predictors of insider espionage and thereby validate the conceptual framework?

With the conceptual framework of insider espionage developed by the researcher in Chapter 4, the next step was to explore its applicability based on actual cases of insider espionage. Yin (2018:175) suggests that matching patterns is one of the most effective techniques for case study analysis. In political science, this technique is also referred to as the congruence method. The technique involves comparing empirically based patterns that were predicted before the case data was collected. Yin (2018:175) suggests further that similarities in the predicted and the empirical patterns are an indication of internal validity. In this study, the predictions are based on the conceptual framework developed by the researcher in Chapter 4 and the empirically based patterns will be based on the data contained in the cases discussed in Chapter 5. Having used the sampling approach outlined in Section 2.3.3, the researcher has selected four cases of insider espionage for analysis: 1) Oleg Gordievsky, 2) Aldrich Ames, 3) Brian Regan, and 4) Edward Snowden. These cases will be discussed in detail in the following subsections.

5.2 CONVENTIONAL INSIDER ESPIONAGE DURING THE COLD WAR: THE OLEG GORDIEVSKY CASE

Oleg Antonovich Gordievsky is a former KGB colonel who had risen through the ranks to become the KGB *Rezident*-designate and bureau chief at the Soviet Embassy in London in 1982. Gordievsky was active as a spy for MI6 from the time of his posting in Denmark in 1974 until he was exposed presumably by Aldrich Ames in April 1985. During this period, Gordievsky provided MI6 with the names of several

Soviet agents who worked in the United Kingdom as well as with insights into various important developments at the highest echelons of the Soviet government. Gordievsky was recalled to Moscow under the suspicion of treason in May 1985. Whilst in Moscow, Gordievsky was allowed free movement even though he was still under investigation. In July 1985, MI6 was able to exfiltrate Gordievsky from the Soviet Union to the United Kingdom via Finland and Norway. He was subsequently sentenced to death *in absentia* by a Soviet court. However, the sentence was never carried out (Andrew, 2009:725-726; MacIntyre, 2018:58; U.K. Parliament, 2021:n.p.).

5.2.1 Personal background

Oleg Gordievsky was born in Moscow on 10 October 1938 as the younger of two sons of Anton Gordievsky and Olga Nikolayevna Gornova. Oleg Gordievsky's father, began his career as a teacher, eventually joined the Communist Party, and became a 'dedicated, unquestioning communist, [and] a rigid enforcer of ideological orthodoxy' (Gordievsky, 2018:47-48; MacIntyre, 2018:8). It was in 1932 that Anton left his career as an educator and moved to Ohrenburg, Kazakhstan, at the behest of Communist leadership where he was responsible for organising the expropriation of food from the local peasants (Gordievsky, 2018:49).

> 'Because this was a brutal operation, often carried out violently, he never cared to speak about it in detail, but essentially it consisted of the forcible seizure of grain, which was needed to feed the army and the population of the big cities where the Bolsheviks were strongest' (Gordievsky, 2018:49).

An estimated 1.5 million people starved to death because of this operation. Anton, however, never wavered in his devotion to the Communist Party. The Party was supreme and, in his view 'always right' (Gordievsky, 2018:49 & 58; MacIntyre, 2018:8). During his assignment in Kazakhstan, he joined the office of state security, and later the Peoples' Commissariat for Internal Affairs (NKVD), which was the precursor of the KGB (Gordievsky, 2018:56; MacIntyre, 2018:8).

Anton's performance in Kazakhstan was evidently deemed satisfactory. He was subsequently made the deputy leader of an expedition to Georgia, where the objective was to assess the agricultural potential of a region that was considered a valuable source of fruit, tea, and cotton. It was during this assignment that he met

Olga Nikolayevna Gornova. The couple began living together and returned to Moscow where, in 1933, Olga gave birth to Vasili, their first child (Gordievsky, 2018:53; MacIntyre, 2018:8). The Gordievsky family thrived in the Stalinist system. It was during this period that Stalin declared that the Communist Revolution was being undermined by traitors and its very existence was in jeopardy.

Anton Gordievsky stood ready to combat the 'subversives'. From 1936 to 1938, Stalin's 'Great Terror' led to countless arrests, imprisonments, deportations to Siberian gulags, and often to the executions of individuals who were merely suspected of being 'enemies of the state'. To many living in the Soviet system, it seemed that the 'safest way to ensure survival was to denounce someone else' (Gordievsky, 2018:56; MacIntyre, 2018:8).

Olga Gordievsky, Oleg's mother, was far less convinced by the Soviet system. She never became a member of the Communist Party, and she quietly questioned the supposed infallibility of the NKVD. The communists had, after all, dispossessed her father's water mill and sent her brother to a Siberian gulag for his criticism of collective agriculture. She witnessed many of her friends being taken away in nightly raids and arrested, never to be seen again. Having grown up as a peasant, she knew how capricious and vindictive state terror could be (MacIntyre, 2018:9). Oleg Gordievsky later wrote:

> My mother was far too sensible to accept propaganda at face value. Being brainwashed by going to an office or sitting through in terminable speeches at party meetings and seminars, she retained the sense of proportion and realized that there could not possibly be as many genuine enemies of the people as the authorities were claiming: criminals and traders simply could not exist in such numbers. Yet when she protested to my father, he brushed her worries aside and sometimes became indignant. He would quote the slogan, 'the NKVD is always right!', he claimed that there must be some good reason behind every arrest. Much later, when I asked him about the techniques of the NKVD in those days, he would say, 'Oh, I understand the main method was recruiting agents, or secret informers'. (Gordievsky, 2018:57-56).

During his school years, Oleg excelled in history and languages, and was indoctrinated in learning the tenets of communist orthodoxy and about the heroes of communism in the Soviet Union and abroad. Despite the 'thick veil of disinformation' regarding the West, he developed a keen interest in foreign countries and, by 1945, began reading 'British Ally', a propaganda sheet distributed by the

British embassy (Gordievsky, 2018:67-68; MacIntyre, 2018:10). In elementary school, Oleg was inducted in the Young Pioneers and at age fourteen, he became a member of the Young Communist League ('Komsomol') (Gordievsky, 2018:89-90).

To those around them, the Gordievskys appeared to be model Soviet citizens: ideologically aligned and loyal beyond doubt to the Communist Party and the state. They 'were well fed, privileged and secure' (MacIntyre, 2018:9). This image remained throughout Oleg Gordievsky's childhood and adolescence. In Oleg's view, this was, however, a façade. The opposing viewpoints that existed among the adults in his family, his father, mother, and maternal grandmother, were never discussed openly. Oleg's father also never spoke of the atrocities in which he was involved. He was an obedient state servant who Oleg later came to see as 'a frightened man'. His mother, critical of the system, 'exuded a quiet resistance that only revealed itself in waspish, half-whispered asides' (MacIntyre, 2018:9-10). Religious worship was illegal in Soviet Russia and the boys were raised as atheists. Nevertheless, their maternal grandmother, a Russian Orthodox Christian, had Oleg's older brother, Vasili, secretly baptised and would have done the same with Oleg if the boys' horrified father had not found out. Beneath the surface, the family was fraught with layers of deception (MacIntyre, 2018:9).

Oleg's experience in the Communist youth organisations caused him to begin questioning the system:

> My early experience in the Young Pioneers and the Komsomol opened my eyes to the way in which the Communist Party worked. I learnt that it was an authoritarian organization run entirely by the leadership, a body in which no ordinary member had any say. I saw that in the Soviet Union there was no democracy, no free elections, and no chance of anything unpredictable happening in the political field. Nobody was allowed to suggest a different candidate; nobody could start up a faction; nobody could propose alternative ideas. Anyone who tried to do so would be quickly suppressed and destroyed. With all its protocols and secret ballots, Soviet political life was a series of dead rituals. And yet, extraordinarily, throughout all seventy-odd years of the Soviet era, the authorities managed to preserve a facade of democracy (Gordievsky, 2018:90).

It was during this period that Oleg Gordievsky also witnessed the appalling treatment of Jews in the Soviet Union. This proved to be an experience that further shaped his views of the Soviet system (Gordievsky, 2018:81-82). Despite his misgivings, Oleg became an accomplished product of the system, excelled in school with top grades, received several gold and silver medals for scholarship, and gained access to university (Gordievsky, 2018:92).

After his graduation from secondary school, Oleg enrolled at the Moscow State Institute of International Relations where he studied history, geography, economics, and international relations, 'all through the warped prism of communist ideology' (MacIntyre, 2018:11). The institute was run by the Ministry of Foreign Affairs and was the Soviet Union's premier educational institution for training diplomats, scientists, economists, politicians, and KGB officers (MacIntyre, 2018:11). It was soon after he began his studies that the Hungarian uprising was beaten down by Soviet forces (MacIntyre, 2018:11).

During his time at the Institute, Gordievsky became close friends with Stanislaw 'Standa' Kaplan who was from Czechoslovakia (MacIntyre, 2018:12). The two men shared similar interests and points of view. Gordievsky writes:

> 'He, too, was liberal-minded, and held strongly sceptical views about Communism, which he was not afraid to express when in the right company' (Gordievsky, 2018:144).

In 1961, between his fifth and sixth year at the Moscow State Institute of International Relations, Oleg Gordievsky was posted in East Berlin for six months. Immediately on his arrival in East Berlin, he witnessed the building of the Berlin Wall first-hand (Gordievsky, 2018:14). Upon his return to Russia, he met Yelena Akopian who was training to be a German teacher. They were eventually married and in 1963, Oleg joined the KGB and had his first tour abroad as a KGB officer in Copenhagen from 1966 to 1970. His tasks in Copenhagen were largely administrative: 'leaving money or messages at dead drops, monitoring signal sites, and maintaining clandestine contact with the undercover spies, most of whom he never met face to face, or knew by name' (MacIntyre, 2018:26). In contrast with his colleagues who 'spent all their time on fishing trips, shopping, and amassing as many material possessions as they could', Gordievsky was absorbed by Western culture. He appreciated Bach and Hayden, and was deeply impressed by Denmark's people, parks, music, and liberties. He loved the country (MacIntyre, 2018:28). It was during his posting in Copenhagen in 1968 that Alexander Dubček, the First Secretary of the Czechoslovakian Communist Party set a new, more liberal course for his country and Warsaw Pact troops invaded Czechoslovakia to crush this movement (Gordievsky, 2018:213; MacIntyre, 2018:31).

From 1970 to 1972, he was assigned to KGB Directorate S, which was responsible for handling Illegals (i.e. operatives without official cover) and he was posted in Copenhagen for the second time in 1972, where he was now a political intelligence officer (MacIntyre, 2018:14 & 45). During that period, he became Deputy Rezident (i.e. Deputy Head of KGB station) (MacIntyre, 2018:46). His marriage with Yelena was failing and it was during this period that Gordievsky met Leila Aliyeva, who had been working as a typist at the World Health Organization in Copenhagen. They started an affair and planned to get married after Gordievsky 'disentangled' his personal situation (Gordievsky, 2018:260).

In 1978, Gordievsky returned to Moscow where he was considered for the post of deputy head of the Third Department of the First Chief Directorate. However, because of his impending divorce – a situation generally frowned upon by the KGB - he was assigned to Partcom (a kind of second personnel department) and as a senior officer 'running important errands' (Gordievsky, 2018:266 & 269). Yelena and Oleg were divorced soon after (Gordievsky, 2018:256).

Gordievsky eventually recovered from the set-back in his career and in 1982, he was posted in London. In April 1985, Gordievsky was promoted to London station chief, but was exposed as an MI6 spy by Aldrich Ames and was recalled to Moscow in May 1985 where he remained under investigation until his extraction by MI6 in July 1985 (MacIntyre, 2018:viii & 2).

5.2.2 Triggers

In some instances, it is a single event or an ongoing situation that triggers an act of insider espionage. In the case of Oleg Gordievsky, however, there were four (4) events that cumulatively pushed him to become an insider spy: 1) the treatment of Jews in the Soviet Union under Stalin in 1952, 2) the Soviet suppression of the Hungarian Uprising in 1956, 3) the building of the Berlin Wall in 1961, and 4) the Soviet suppression of the Prague Spring in 1968.

Recalling Stalin’s actions against Soviet Jews in the early 1950s, Gordievsky wrote:

> ‘My political awareness, already precocious, was much heightened by an event that took place in the autumn of 1952, when I was not quite fourteen. Several prominent doctors were arrested together in Moscow, accused of the murder of Zhdanov, Sherbakov and other leading Communists. Everyone suspected that the case was a sham for of the fifteen or so general practitioners seized, all but one were Jewish, and the operation was obviously an anti-Jewish plot hatched by Stalin. The woman who wrote the denunciation, Lydia Timashuk, was ostentatiously decorated, and other Jews started to lose their jobs.
>
> I followed all this with close interest but then, suddenly, the anti-Semitic operations of the government came closer to home. In a flat across the landing from ours lived a Jewish family, father, mother and child. The father was a lieutenant colonel in the KGB, deputy head of the medical centre, and the mother was a major, head of the Party organization. Both had joined the Party in the 1920s and served it loyally, two among thousands of Jews who hoped that the Communists would win political rights for their race and open up real possibilities for them. Unlike many Russians, who merely paid lip- service to Communism, these two strongly believed in the system and now lost their jobs simply because they were Jews. The same thing happened to another family on the ground floor of our block. The father, a major, had a boy about Marina's age- they were the first people in our block to own a television set, and they kindly let me watch it for an hour or so in the evenings. That man also lost his job for no reason: he went to Kiev, where he hoped life would be easier, and I never saw him again. Young as I was, I could not help being struck by the stupidity and injustice of these dismissals. The people involved were clever, dedicated, and serious specialists who had lost their livelihoods because of their racial origins. I began to feel critical of a system which could treat innocent citizens so badly’ (Gordievsky, 2018:81-82).

After Stalin’s death and the ensuing power struggle in 1953, Nikita Khrushchev became the First Secretary of the Communist Party of the Soviet Union. After three years (i.e., during the 20th Party Congress), Khrushchev denounced Stalin and condemned the former dictator’s crimes. A modest relaxation of Soviet repression and censorship followed. Khrushchev’s de-Stalinisation policies also saw millions of political prisoners released from the gulags (Khrushchev, 1971:347-349). The ‘Khrushchev Thaw’ had begun.

Old hardliners such as Anton Gordievsky, were stunned by these new developments. The young Oleg Gordievsky, however, was inspired and hopeful that the country would now move towards greater freedom and democracy. Much to his disappointment, the limits of the ‘Khrushchev Thaw’ soon became visible when

Soviet tanks rolled into Hungary to suppress a nationwide uprising (MacIntyre, 2018:11). Oleg Gordievsky summarises his experience as follows:

> '… within a few days our new-found freedom was abruptly curtailed: in the last week of October Hungary rose in revolt against Soviet oppression, only for the rebellion to be brutally crushed by tanks rolling into the heart of Budapest. It was hard for us to discover exactly what had happened, since the official propaganda was overwhelming. The Soviet press reported that there had been a Fascist rebellion and that, in an action of fine proletarian solidarity, Soviet troops had gone in to help the long-suffering Hungarian people. The scraps of genuine news which I managed to pick up on our primitive shortwave radio told a different story but it was impossible to form a coherent picture of events.
>
> Nevertheless, even in Moscow it was soon apparent that a terrible disaster had occurred, for our temporary release from censorship ended overnight. The atmosphere changed entirely: all warmth disappeared, and an icy wind set in. Life, in other words, returned to normal: we had gone back into the cold, and all the thousands of 'Homo sovieticus' carried on as they had before, toeing the Party line' (Gordievsky, 2018:98-99).

In 1961, between his fifth and sixth year at the Moscow State Institute of International Relations, Oleg Gordievsky was permitted to spend six months in East Berlin to gain practical experience in a foreign country. There were sixty (60) students in Gordievsky's class and half of them could go abroad. The other half would spend time either at the Ministry of Foreign Affairs, or at a news agency such as TASS (Gordievsky, 2018:121).

On the 13th of August 1961, the day after his arrival in East Berlin, Gordievsky knew that a massive operation had just been launched by the East German government at the behest of Moscow to build a wall separating the Soviet-occupied part of Germany from the West. The official East German and Soviet narrative was that the wall was being built to protect the East from fascist Western influence. But, in reality, it was 'a prison perimeter, erected by East Germany to keep its own citizens penned in' (MacIntyre, 2018:15). One hundred and fifty miles of concrete wall, vehicle obstacles and barbed wire fencing, became the physical symbol of the Iron Curtain. This was yet another event that had a profound effect on Gordievsky and his disillusionment with Communism and the Soviet state. Gordievsky writes:

> In a personal sense, the building of the Wall was a bitter blow to me as it meant that I could not visit the Western half of Berlin or see any of the sights on which I had set my heart: Charlottenburg, the Kurfürstendamm, the Tiergarten, the Olympic stadium. At weekends, though, we were

> allowed to take a commuter train and travel out to any destination within half an hour of the city centre among the lovely lakes and woods to the east and south.
>
> The Wall had a far more profound effect on me than that of restricting physical movement: it stimulated another leap in my mental development. At first hand I saw how repugnant Communism was to ordinary people. I saw that only a physical barrier, reinforced by armed guards in watch-towers, could keep the East Germans in their socialist paradise and stop them fleeing to the West. For the first time I saw what the Soviet Union was doing to Eastern Europe' (Gordievsky, 2018:132).

In January 1968, Alexander Dubček, the First Secretary of the Czechoslovakian Communist Party charted a new course for his country. The reforms included ushering in greater liberties for its citizens, relaxing travel restrictions, allowing free speech, and doing away with censorship. The changes also included curtailing the powers of Czechoslovakia's secret police, improving relations with the West, and plotting a course to free elections. Oleg Gordievsky saw these developments as a hope for a more liberal future in Eastern Europe, not just in Czechoslovakia, but in the Soviet satellite states and in the Soviet Union as well (Gordievsky, 2018:213; MacIntyre, 2018:31).

Soviet tanks and troops were amassed along the Czechoslovakian border. At the Copenhagen KGB *rezindentura*, where Gordievsky was based at the time, opinions were divided as to the Kremlin's next move. Some were certain that the Soviet Union would suppress the liberalisation process in Czechoslovakia by force. Others, such as Gordievsky, were convinced that Soviet leadership would not use force to quell the Czechoslovakian reforms. In Moscow, however, the developments in Czechoslovakia were seen as an 'existential threat to communism itself' which could potentially 'tip the balance of the Cold War against Moscow' (MacIntyre, 2018:31).

On 20 August 1968, 2000 tanks and more than 200,000 Soviet troops and other Warsaw Pact states crossed the border into Czechoslovakia. The country was occupied, and the reform was crushed. The Soviet operation under the Soviet Union's leader Leonid Brezhnev, was adamant that any Warsaw Pact country that attempted to renounce orthodox communism and introduce liberal policies would be compelled to comply (MacIntyre, 2018:33). Gordievsky's thoughts were with Standa Kaplan, his good Czechoslovakian friend from the Moscow State Institute of

International Relations. He could only imagine what Standa might have been thinking (MacIntyre, 2018:34).

Oleg Gordievsky valued political, cultural, and spiritual freedom, democracy, and prosperity in his adulthood (Gordievsky, 2018:11). The treatment of Jews in the Soviet Union under Stalin, the Soviet suppression of the Hungarian Uprising, the building of the Berlin Wall, and the Soviet suppression of the Prague Spring were all events that conflicted with these values (Gordievsky, 2018:81-82, 98-99, 132, 213). It was the Soviet Union’s attack on Czechoslovakia’s effort to introduce liberal reforms that finally led Oleg Gordievsky to the breaking point (Gordievsky, 2018:213).

5.2.3 Motives

Actions initiated by the Soviet leadership stood in complete opposition to Gordievsky’s values. He regarded the Soviet system as oppressive and lacking any orientation towards freedom or democracy. Moreover, through the events surrounding the Khrushchev Thaw and the Prague Spring he concluded that any attempts to introduce liberal reforms would be swiftly and decisively crushed. Gordievsky found this to be deeply offensive (Gordievsky, 2018:81-82, 98-99, 132, 213).

Gordievsky’s contempt for the Soviet system and state grew stronger with each event that violated his core values. Following the invasion of Czechoslovakia, Gordievsky could no longer contain his rage (Gordievsky, 2018:213). As infuriated Danish protesters gathered outside the Soviet embassy in Copenhagen to protest the Soviet invasion, Oleg Gordievsky felt deeply ashamed of being associated with the Soviet system (MacIntyre, 2018:34). Gordievsky writes:

> ‘As the world knows, the invasion went ahead on the morning of 21 August; and it was that dreadful event, that awful day, which determined irrevocably the course of my own life. Over the past two years I had become increasingly alienated from the Communist system, and now this brutal attack on innocent people made me hate it with a burning, passionate hatred. 'Never again will I support it,' I told myself. 'On the contrary, from now on I must do everything I can to fight it.' Even as the tanks were smashing their way into Prague, I rang Yelena from the booth in the main hall of the Embassy, on a line which I knew was bugged by the Danes, and cried, 'They've done it! It's unbelievable. I just don't know what to do’ (Gordievsky, 2018:213).

Oleg Gordievsky was infuriated and seriously contemplated ways in which he could fight the Communist system. He writes:

> ‘As for my own future course of action, I could not immediately see what to do. When I went back to Moscow, I thought, I would write and circulate truthful reports which would reveal the facts about NATO: that the West had no aggressive intentions against the Soviet Union, and that on the Soviet side propaganda was affecting even those who were supposed to be making realistic political assessments. Then I saw how childish any such idea was: to try to organize underground cells in Russia would be futile, for the domestic KGB would penetrate them at once’ (Gordievsky, 2018:214).

At this point, Gordievsky had not yet devised a plan how to proceed. It was clear, however, that he was no longer willing to be one of the countless Russians who secretly despised the system but failed to act. He decided that he would have to change jobs and become involved in political intelligence, which would allow him to be closer to the front where he would be able to collect intelligence himself. From this point forward, Oleg Gordievsky was ready to act (Gordievsky, 2018:214-215).

5.2.4 Situational vulnerabilities

In his further analysis, Gordievsky could detect several vulnerabilities in the KGB security setup that could be exploited and would enable acts of espionage. Clear desk policies and document storage policies are two important elements of information security (Prunckun, 2019:131). At the KGB *rezidenturas,* telegrams from Moscow were well protected and could not be taken from the areas in which they were stored. To perform their tasks, the KGB officers would have to take notes while reading the telegrams. These notes, however, could be taken along and were apparently not traced or accounted for.

Moreover, every two weeks, a courier would bring messages from Moscow in the form of a microfiche film. The *Rezident* would read the film, and then cut and distribute segments of it to the KGB officers responsible for dealing with the information in the respective segments. During the lunch breaks and at the end of the day, the cipher clerks were required to collect and store all sensitive materials including the microfiche films (Gordievsky, 2018:196 & 256-257). In practice, however, the cipher clerks never collected and stored these materials during the lunch breaks. Instead, while they were out for lunch, the KGB officers would store the sensitive materials in briefcases that they would leave on their desks or in steal lockers in their offices. While cipher clerks were permitted to enter and retrieve sensitive materials from the offices in the absence of the KGB officers, they practically never did so (Gordievsky, 2018:257).

Having security personnel searching the offices, bags, pockets, and other items is a common practice in physical security. At the KGB *rezidentura,* cipher clerks were permitted to search the briefcases that KGB officers left on their desks during their lunchbreaks. In addition, staff entering and leaving the Soviet embassy premises could be subject to spot-checks by security personnel. However, in practice, these spot-checks very rarely took place. This proved to be a further vulnerability in the KGB security system. Gordievsky could – at least for brief periods during his lunch break – leave the *rezidentura* with a variety of materials including the microfiche films (Gordievsky, 2018:257).

5.2.5 Market opportunities

There is no complete publicly available inventory that shows what information Oleg Gordievsky provided to MI6. What is known, however, is that he provided the solution to an enigma that had baffled Canadian and British intelligence officials since the defection of KGB cipher clerk Igor Gouzenko in 1945. According to evidence that Gouzenko provided to Canadian officials while he was stationed in Ottawa, there were two (2) Soviet agents codenamed ELLI working in the British government. One was immediately identified as Kay Willsher, the deputy registrar at the British High Commission in Ottawa. The identity of the other, Leo Long, an intelligence officer with British Scientific Intelligence (MI16) and later with the Control Commission in Germany until 1952, remained unknown until Gordievsky uncovered the secret in 1982 (Andrew, 2009:350-351; Parliament UK, 1981:n.p.).

Gordievsky was also instrumental in shedding light on the defection of Bruno Pontecorvo. Pontecorvo was an Italian-born atomic physicist who began working with a wartime Anglo-Canadian atomic research team in Montreal in 1943 and was later working at a Harwell research centre in the UK. It was eventually discovered that Pontecorvo and his wife were communists and, therefore, security risks. In 1950, before an investigation could be launched, Pontecorvo and his wife defected to the Soviet Union. While Pontecorvo was known to have been a defector, it was not until 1982, through the disclosure of Oleg Gordievsky, that British officials learned that Pontecorvo was, in fact, a spy who had offered his services to the Soviets and who was held in high esteem by his Soviet handlers for the information he was able to provide (Andrew, 2009:391-392).

The identity of the fifth man in the Cambridge Spy Ring had long eluded British intelligence. It was through the help of Oleg Gordievsky that the connection could be made between the unknown fifth man and John Cairncross, a British intelligence officer, who had confessed his role as a Soviet spy some years' prior (Andrew, 2009:440-441). Gordievsky also unmasked the Member of Parliament, Bob Edwards, union leader Jack Jones, and MI5 counterespionage officer Michael Bettaney who were active KGB agents (Andrew, 2009:710 & 714). While all these insights were certainly welcomed by MI6, there were two (2) contributions provided by Gordievsky that arguably changed the course of world history. During the year prior to his death, the Soviet leader and General Secretary of the Communist Party of the Soviet Union, Yuri Andropov, had become increasingly paranoid about developments in the West. The anti-Soviet rhetoric of U.S. President Ronald Reagan and the British Prime Minister Margaret Thatcher raised the fear that they were planning a strike against the Soviet Union. This impression was exacerbated by the annual NATO command-post exercise ABLE ARCHER in 1983, which simulated an escalation of hostilities between NATO and Warsaw Pact forces. Unaware of the Soviet trepidations, the exercise was to culminate in the US military simulated DEFCON 1 and coordinated nuclear attack against the Soviet Union. Soviet officials were increasingly convinced that an actual first-strike nuclear attack from the West was imminent. Oleg Gordievsky learned of the fears among Soviet leaders and reported this to his MI6 handlers. The information reached the two (2) Western heads of government who subsequently initiated measures to de-escalate the situation before it became worse and uncontrollable (Andrew, 2009:722-723).

It was also Oleg Gordievsky who anticipated the rise of Mikhail Gorbachev, as leader of the Soviet Union and General Secretary of the Soviet Communist Party, well before his assumption of these offices. This gave Prime Minister Thatcher the opportunity to lay an early foundation for a more constructive dialogue between

Britain and the Soviet Union during Gorbachev's visit to the United Kingdom in December 1984. While briefing MI6 about the internal developments leading up to Gorbachev's rise to power, Gordievsky was also informing the KGB and ultimately Gorbachev himself about the positive change in British posture towards the Soviet Union and the person of Mikhail Gorbachev. Gordievsky's actions were considered to have been instrumental in easing relations between the two sides of the iron curtain (Andrew, 2009:725).

While money is the principal incentive for insider espionage, this was clearly not Oleg Gordievsky's motivation. During the initial meeting with his handler, Gordievsky told him that he wanted 'No money. I want to work for the West out of ideological conviction, not for gain' (MacIntyre, 2018:67). Gordievsky did eventually agree to accept money from MI6, but had it deposited in a London bank and earmarked it for an emergency if he had to defect to the West (MacIntyre, 2018:82).

5.2.6 Disinhibiting factors

Throughout his adolescence and adulthood, Oleg Gordievsky had come to be profoundly critical of the Soviet system. He considered it to be totalitarian, oppressive, and inhumane (Gordievsky, 2018:123). He valued and believed in freedom, democracy, and justice. The events that triggered his outrage with the Soviet system also fuelled his rebellion. The treatment of Jews in the Soviet Union, the Soviet suppression of the Hungarian uprising, and the building of the Berlin Wall were events that deeply violated his values. But it was the 1968 Soviet-led Warsaw Pact invasion of Czechoslovakia during the Prague Spring that brought on his fury against the Soviet system and his shame in being a part of it (Gordievsky, 2018:81-82, 98-99, 132, 213). He later explained that the Warsaw Pact invasion of Czechoslovakia had 'irrevocably' changed the course of his life. Although he had already become increasingly disaffected with the Soviet system during the years before the invasion, it was the brutality of the attack on the innocent people of Czechoslovakia that invoked his hatred. He became so passionate in his detestation of the Soviet system that he swore never to support this system again and to do all he could to fight it (Gordievsky, 2018:213).

After a failed first attempt to establish contact with Western intelligence during Gordievsky's first posting in Copenhagen in 1968, he finally succeeded in establishing contact with British intelligence during his second posting in Copenhagen in 1974. MacIntyre summarises the moment in which Gordievsky finally and irreversibly decided to work with his MI6 handler:

> 'In that one cathartic moment, in the corner of a Copenhagen hotel, all the strands of a long-brewing rebellion had come together: his anger at his father's unacknowledged crimes, his absorption of his mother's quiet resistance and his grandmother's hidden religious beliefs; his detestation of the system he had grown up in and his love of the Western freedoms he had discovered; his shimmering outrage over the Soviet repressions of Hungary and Czechoslovakia and the Berlin Wall; his sense of his own dramatic destiny, cultural superiority and optimistic faith in a better Russia. From now on, Oleg Gordievsky would live two distinct and parallel lives, both secret and at war with one another. And the moment of commitment can with the special force that was central to his character: an adamantine, unshakable conviction that what he was doing was unequivocally right, a whole-souled moral duty that would change his life irrevocably, a righteous betrayal' (MacIntyre, 2018:58).

From this point onward, Oleg Gordievsky could weaken the Soviet system which he so detested and repeatedly strike a blow against what he regarded as Soviet tyranny (Gordievsky, 2018:58, 196, 213 & 256-257).

5.3 INSIDER ESPIONAGE DURING A PERIOD OF GEOPOLITICAL AND TECHNOLOGICAL TRANSITION: THE ALDRICH AMES CASE

Aldrich Hazen 'Rick' Ames was a CIA intelligence officer from 1967 until his arrest and prosecution in 1994. Ames and his wife, Maria Del Rosario Casas Ames, were charged with espionage for the Soviet Union and its successor, the Russian Federation (Bromwich, 1997:n.p.). The Ames case 'represented a security breach of disastrous proportions,' forcing the CIA to shut down numerous operations and causing the incarceration and, in some instances, the execution of CIA assets in Russia (Earley, 1997:143; Senate Select Committee on Intelligence, 1994:2). Shortly after their arrests, Ames and Rosario entered a plea bargain in exchange for their full cooperation. The couple's assets, amounting to US$547,000, were subsequently transferred to a victims' assistance fund. Ames was consequently imprisoned for life without the possibility of parole, while Rosario Ames was sentenced to a 63-month jail term, which allowed her to continue raising their son after serving her sentence (Federal Bureau of Investigation, 2021:n.p.).

5.3.1 Personal background

Ames was born in River Falls, Wisconsin, on May 26, 1941. His father, Carleton Cecil Ames, held a doctorate and taught at River Falls State Teacher's College. During this period, Ames' mother, Rachel, was an English teacher at a local high school. Aldrich Ames' sisters, Nancy and Alison, were born in 1942 and 1945 respectively. Aldrich Ames' father joined the CIA in 1952. The Ames family moved to Virginia, where Rachel Ames began working as an English teacher in the Fairfax County public school system. The elder Ames was assigned to an overseas tour in Southeast Asia from 1953 to 1955. His family, including Aldrich, joined him on this tour (Senate Select Committee on Intelligence, 1994:4).

Aldrich Ames describes his childhood as a happy one, but with clear behavioural guidelines:

> ‘My parents always seemed super-busy and happy. I don't remember any tense times. On weekends, we'd pile in their bed in the mornings and Dad would read the comics. But manners! Oh, manners! There was absolutely no talking back, no door-slamming, and we learned that Dad didn't buy every fad toy. I remember my bitter disappointment when ‘all the kids’ had blue Civil War-style forage caps and Dad refused to buy me one. He said a fad was no reason at all, that being like all of the other kids was not something to aim for.
>
> I was told that I was a good child, but, of course, I had faults. I was caught stealing a candy bar at O'Brien's Cafe the adult hangout on Main Street, and Dad marched me down to return the candy bar and to apologize to Mr. O'Brien personally. I never shoplifted again. Another time, I shot out the elementary school principal's car side windows, all four of them. It was on my birthday and I used my brand- new Red Ryder BB gun, which I never saw again’ (Ames quoted in Earley, 1997:25).

Carleton and Rachel Ames also impressed a variety of other beliefs and values on Rick Ames and his sister:

> ‘Mom and Dad always impressed us with the need for manners, ideas, integrity. They were friends with the only Jewish couple in town, and I remember Dad explaining to me about Jews, anti-Semitism, and the evil of prejudice. When I saw a black man for the first time in St. Paul, Dad told me about slavery and discrimination. There was also a flavour of being not better than others, but being held to different, and implicitly higher, standards. I see it almost as a class distinction now, though Mom and Dad were devoid of what could be called snobbishness or reserve, much less pretending to be from better origins. The idea was that individual integrity and worth was of paramount importance. Also, independence, and a refusal, the way I got it anyhow, to whine, beg, draw

> attention to oneself, brag, or push forward. Stoicism was the virtue, and one's own efforts and sense of value sufficient reward. Praise, though we got it and knew our parents' pride in us, was worth nothing by itself, and shouldn't be pursued for its own sake' (Ames quoted in Earley, 1997:25).

Carleton Ames also had a strong influence on Aldrich Ames' political ideologies. World events were often the topic of conversation during family meals. Carleton Ames was an ardent and vocal critic of communist regimes, which he considered to be inhuman and dehumanising. During one family dinner he stated that he would rather see his family dead than living under communism. Aldrich Ames shared many of his father's views. He was and remained equally critical of the communist system (Cherkashin & Feifer, 2005:28; Earley, 1997:28). However, shocked by his father's extreme view, the young Aldrich could not agree that being dead was preferable to living under communism. In Aldrich's view, '[r]egardless of the amount of human cruelty and brutality under communism, we all share a common humanity, whether we were the oppressed or the oppressors' (Earley, 1997:28).

Carleton Ames was also an important influence in Aldrich Ames' life in another regard. The elder Ames developed a serious alcohol dependency that had an effect, both on his private and his professional life. During the tour in Southeast Asia, matters came to a head when he received a particularly negative performance appraisal. When he returned to the United States, the elder Ames was placed on a six-month probation period that he managed to pass, but he was never again entrusted with a foreign-based assignment (Senate Select Committee on Intelligence, 1994:4).

In 1957, Carleton Ames arranged for his son, Aldrich to be hired by the CIA as a summer hire. Aldrich was in his sophomore year (tenth grade) in high school at that time and his work involved marking classified documents for filing. Aldrich returned to work for the CIA during the following two summers. Upon his high school graduation in 1959, he registered at the University of Chicago with the intention of completing a degree in history while following his long-time passion for drama. In the summer of 1960, the CIA hired him as a labourer/painter. He returned to the University of Chicago for the autumn semester in 1960 but had to leave school because of his failing grades. Ames subsequently went to work as an assistant technical director at a Chicago theatre. In early 1962, he reapplied for employment with the CIA, this time as a full-time employee, and was hired to perform the same type of work that he did some years earlier as a high school student. While working for the CIA, Ames completed his degree in history with a B- average in 1965 (Senate Select Committee on Intelligence, 1994:4-5).

In 1967, Ames applied for and was accepted into the CIA Career Trainee Program. Two years later, Ames married a fellow CIA officer, Nancy Segebarth. Soon after, Ames was offered his first foreign assignment in Ankara, Turkey, where he was based from 1969 to 1972. Since CIA policy prohibits spouses to be working as intelligence officers in the same office, Nancy Segebarth resigned from the CIA to accompany her husband to Turkey. While the couple was based there, the CIA employed Nancy in her husband’s office to perform part-time administrative work (Senate Select Committee on Intelligence, 1994:5).

During the first year of his assignment in Turkey, Aldrich Ames’ work performance was rated as ‘strong’, which led to his promotion to the grade of GS-11 in 1970 (Senate Select Committee on Intelligence, 1994:6). However, his marriage began to fall apart. According to Aldrich Ames’ own account, the couple was still getting along during this time, but they were beginning to lose interest in each other and decided that they did not want children together. Similar to his father, Aldrich Ames had developed an increasingly serious drinking problem which had adverse effects on his work and marital life. On one occasion, Ames overindulged at a party that the couple was invited to. His wife felt embarrassed by his actions and was henceforth troubled by Aldrich’s drinking habits. She admonished him whenever he ‘even had two drinks at a party after that’ (Earley, 1997:53-54). During the years that followed, Ames’ work performance steadily declined and during his last year in Turkey, his superiors ‘considered him unsuited for field work and expressed the view that perhaps he should spend the remainder of his career at CIA Headquarters in Langley’ (Senate Select Committee on Intelligence, 1994:6).

When the couple returned to the United States in 1972, Ames’ wife became deeply involved in community politics (Earley, 1997:53). Ames’ work performance improved. He eventually received offers for overseas assignments again, which he repeatedly declined because he did not want to put further strain on his marriage. He realised, however, that frequent rejections of overseas assignments would eventually jeopardise his CIA career. So, in September 1981, he finally accepted an assignment in Mexico 'where he believed he could stay in fairly close contact with his wife', who had decided to remain in New York (Senate Select Committee on Intelligence, 1994:7).

During his assignment in Mexico, Ames' initial performance was satisfactory, but as in Ankara, it eventually began to decline. While he left for Mexico with the hope of being able to salvage his marriage, he realised, in time, that he was no longer sufficiently committed (Senate Select Committee on Intelligence, 1994:7). Nevertheless, his need for companionship remained and by the end of 1982, Ames had been involved in three extramarital affairs. It was during this period that Ames met Maria del Rosario Casas Dupuy, the cultural attaché at the Colombian Embassy in Mexico City. Throughout the following year, Ames' relationship with Rosario became increasingly serious (Senate Select Committee on Intelligence, 1994:7 & 11).

5.3.2 Triggers

In October 1983, Aldrich and Nancy Ames formally separated. As a part of the separation agreement, Ames had to pay his estranged wife $300 per month. In addition, he had to pay all the remaining credit card and other debts, which totalled $33,350. Ames was convinced that the separation agreement would bankrupt him. It dealt a severe blow to Ames' sense of financial security and put him under considerable pressure. The situation was further exacerbated by his relationship with Rosario. Ames and Rosario were seriously planning to start a family together. This, however, put even more pressure on Ames whose financial challenges gradually escalated (Senate Select Committee on Intelligence, 1994:11).

In November 1983, a month after his formal separation from Nancy and shortly before his relocation back to the United States, Ames submitted an 'outside activity' report to the CIA in which he formally notified the Office of Security of his relationship with Rosario (Senate Select Committee on Intelligence, 1994:10). From a CIA procedural point of view, this was a clear indication of his level of commitment to Rosario. Then, in April of 1984, Ames notified the CIA of his intention to marry Rosario. He was, at this time, still married to, but legally separated from his first wife.

Five months later, in September 1984, Nancy Ames ‘filed for divorce on grounds of mental cruelty’ (Senate Select Committee on Intelligence, 1994:10).

Ames was happy in his relationship with Rosario, but the problems related to his excessive drinking prevailed. What had adversely affected his marriage with Nancy Ames was now also affecting his relationship with Rosario. In an interview, Ames stated:

> ‘Rosario was used to and enjoyed social drinking, and at first, I don’t think she was alarmed by my habits. In practice, I used her willingness to drink with me as a license to drink freely, without guilt, always stopping short of total drunkenness. I also used to egg her on, but only managed to get her to the point of a social high three times. By 1984, she stopped drinking, except for a glass of wine at dinner or at a party. She said it was because of her weight, but I think it was her attempt to get me to stop. I tried and even promised several times not to drink at home. But I always cheated, sneaking in a bottle of liquor and then concealing it or lying about it. Because Rosario disliked me drinking at home, I took up the practice of drinking alone at lunchtime, when I would consume four or five double vodkas at least once a week, sometimes twice. I really had no choice, since Rosario kept close tabs on me at night. This created problems, because I not only had to hide my drinking from my colleagues at work but also keep it from Rosario’ (Ames quoted in Earley, 1997:113).

At this juncture, Ames was no longer just faced with the pressures of his financial difficulties. Due to his drinking habits, he was now also faced with the risk of an untimely end of his relationship with Rosario. Ames explained:

> ‘Rosario was difficult, conflicted, but it also seemed to me to be a matter of life and death - really. I am being serious here. My failure is with my first wife, my sense of loneliness and alienation from warmth and humanity, all convinced me that if I failed in loving Rosario, only a kind of living death or suicide remained for me’ (Ames quoted in Earley, 1997:146-147).

It was thus, not only his need for (financial) security, but also his need for love and companionship that was under serious threat.

5.3.3 Motives

Ames regarded his situation as being desperate. In a later interview, he concedes that he was overreacting to the situation he was in (Senate Select Committee on Intelligence, 1994:11). However, an important feature of appraisal is that the individual’s perception at the time of the appraisal determines how the individual will respond to an event or situation (Roseman & Smith, 2001:6). Ames was being stretched by conflicting needs (financial security and love/belongingness), and his assessment at that time was profoundly negative (Earley, 1997:113 & 146-147; Senate Select Committee on Intelligence, 1994:11*).* He seemed certain that his life with Rosario would come to an end if he did not find some way to influence the outcome. Ames explains:

> 'Rosario herself was not my salvation, but 'we' would be - but only if there could be a 'we'. I could only survive if I could find a way for us to survive' (Ames quoted in Earley, 1997:146-147).

Ames' financial impasse and the prospect of losing Rosario were deeply troubling and caused him to be profoundly fearful. In retrospect, Ames describes his involvement in espionage as an act of 'cowardice' in the face of the personal and financial losses he was expecting to incur (Earley, 1997:146-147). Fear motivates people to focus their attention on that which causes the fear and to find a way to escape it (Deckers, 2016:389). By his own accounts, Ames was ready to take some sort of action to avert the threat of losing Rosario. Ames had convinced himself that by raising enough money, he would be able to remedy his desolate financial situation and, most importantly, to hold on to his life with Rosario. In his words:

> 'I wanted the cash. But the reason I needed the money was not for the reasons most people want money. I did not want it for a new car or a new house, but rather for what it could guarantee. It seemed to be the only way for me to guarantee that the 'us' I desired so desperately would survive. It would make 'us' possible and, therefore, make our love a lasting one. I wanted a future. I wanted what I saw we could have together. Taking the money was essential to the re-creation of myself and the continuance of 'us' as a couple' (Ames quoted in Earley, 1997:147).

By this time, it had become clear that Ames was ready to act. He had just not yet decided how he was going to raise the money. He seriously considered various options to achieve this objective. The extent of his determination to act becomes apparent through his description of one option in particular that Ames was entertaining: Ames was very seriously planning to rob a bank and only dismissed this option because he felt that it would not allow him to raise enough money (Earley, 1997:134 & 136).

5.3.4 Situational vulnerabilities

Vulnerability is a shortcoming in the security system, security procedures, internal controls, or implementation that can be exploited (National Institute of Standards and Technology, 2021:n.p.). In the case of Aldrich Ames, there were several vulnerabilities that facilitated his acts of espionage. Physical security involves a wide range of security measures including access controls (Frazier, Nakanishi & Lorimer, 2009:29). Such controls, however, were evidently lacking in the case of Aldrich Ames. According to a report of the Senate Select Committee on Intelligence (1994:69), Ames was able to 'visit offices he had no reason to be in and gain access to information he had no business seeing'.

In Ames' case, there was also an issue related to the risk of material being illicitly removed from CIA premises. The CIA had adopted a policy in the late 1970s allowing security personnel to perform unannounced and random searches on every staff leaving the CIA premises. This policy, however, was abandoned soon after because it was considered inconvenient for those being subjected to the searches. By abandoning this policy, the CIA not only deprived itself of the possibility of discovering material that was not to be taken from the premises, but more importantly, it now also lacked an important deterrent to those who might have been considering espionage. In the absence of this policy, Ames could feel safe in removing considerable amounts of material without being detected (Senate Select Committee on Intelligence, 1994:69-70). According to the Senate Select Committee report on the Ames case, the information security system:

> '… demonstrated gaps in the control of sensitive classified information. Ames was able-without detection-to walk out of CIA headquarters and the U.S. Embassy in Rome with bags and envelopes stuffed with classified documents and materials. Many of the classified documents he passed to his KGB handlers were copies of documents that were not under any system of accountability. Ames did not even have to make copies of them' (Senate Select Committee on Intelligence, 1994:69).

During an interview following his arrest, Ames told authorities that his KGB handlers were 'amazed' at the quality and quantity of information he was able to remove from CIA premises without arousing suspicion. The fact that he was able to 'take large bundles of classified information out of CIA offices' demonstrated the laxness of the information security system that the organisation had in place (Senate Select Committee on Intelligence, 1994:69).

Apart from the hard-copy material Ames was able to remove, he later also found ways to exploit vulnerabilities in the CIA cyber system. During his last CIA posting, Ames was assigned to the CIA Counternarcotics Centre in Washington. While working there, he downloaded classified documents onto floppy discs which he could then smuggle from the CIA premises. On one occasion, he was able to put as many as three or four hundred documents on a floppy disc. During this assignment, Ames attended a conference in Rome and brought a lap-top computer along to do work in the unprotected environment of his hotel room. Although other CIA staff were aware of this incident, it apparently did not raise any security concerns (Senate Select Committee on Intelligence, 1994:69 & 121).

Clearly, cyber-protection technologies were not as advanced as they are today. Nevertheless, the recommendations of the Senate Select Committee on Intelligence that examined this case at the time offer an insight into the measures that could have been, but were not in place. These included preventing employees from downloading classified documents onto data storage devices without authorisation and enabling cybersecurity personnel to perform audits of specific computer functions to detect and monitor the actions of agency staff (Senate Select Committee on Intelligence, 1994:70).

5.3.5 Market opportunities

In terms of market value, Aldrich Ames had much to offer. By the time he began entertaining the idea of volunteering his services as a spy to the KGB in late 1984, he had already been a CIA intelligence officer for 15 years. In those 15 years, he was posted in:

- Ankara, Turkey from 1969 to 1972;
- Washington, D.C. from 1972 to 1976;
- New York, N.Y. from 1976 1981;
- Mexico City, Mexico from 1981 to 1983; and
- Washington, D.C. from 1983 (United States District Court for the Eastern District of Virginia, 1997:4).

Ames was assigned to Ankara as a field officer where his job involved recruiting Soviet agents as assets (spies) for the CIA (Earley, 1997:40). In Washington, Ames was assigned to the CIA's Soviet-East European (SE) Division of the Directorate of Operations (DO). While there, he received Russian language training and was then responsible for giving support to CIA field operations against Soviet officials in the United States. From Washington, Ames was transferred to New York and tasked with handling two important Soviet assets for the CIA. In Mexico, Ames' work also involved handling and developing assets (Senate Select Committee on Intelligence, 1994:6-7).

The insights that he could offer after so many years with the Agency made him a high value asset for the KGB and, after the Cold War, Russia's internal Federal Security Service (FSB - F*ederal'naya sluzhba bezopasnosti)*. Ames could furnish his handlers with substantial amounts of documentation, and this made him one of the most important suppliers of intelligence (Senate Select Committee on Intelligence, 1994:69). Moreover, the KGB knew that it had leaks in its system. The fact that Ames was able to provide the identities of many of them made him invaluable. In exchange for the information he delivered, Ames received a total of $2.5 million over the nine-year period of his spy activities (Senate Select Committee on Intelligence, 1994:2).

5.3.6 Disinhibiting factors

When he returned to the United Sates in 1983, Ames' financial situation was bleak. Rosario joined him and the couple lived in a small apartment, owned an old malfunctioning Volvo car, and could barely afford to buy their groceries (Earley, 1997:126 & 130; Senate Select Committee on Intelligence, 1994:11). Making matters worse, Ames felt considerable pressure under the weight of the recent separation settlement with his first wife, Nancy (Earley, 1997:132; Senate Select Committee on Intelligence, 1994:11). Rosario was affected by their money difficulties and began speaking to friends about how much better her life was in Colombia and in Mexico (Earley, 1997:130).

Ames' fear of personal bankruptcy and losing Rosario fuelled his determination to find a way out of his situation (Earley, 1997:135; Senate Select Committee on

Intelligence, 1994:11). He surmised that only by offering Rosario a more comfortable lifestyle would he be able to ensure that they remain together. For this, however, he needed a sufficiently large amount of money (Earley, 1997:147). In his desperation, Ames only considered two options to improve matters. Both were illegal. He first thought of robbing a bank. On reflection, however, he concluded that this would not produce a sufficiently large income and that he would have to rob several banks. The thought of this scared him and so he turned his thoughts to committing espionage (Earley, 1997:134).

Ames explains that his thoughts of committing a crime were initially only 'fantasies' and 'mind games' (Earley, 1997:134). However, when he was unexpectedly served with divorce papers from his first wife in late 1984, charging him with mental cruelty, the pressures on Ames became unbearable (Earley, 1997:134). According to the Senate report on the Ames case, it was these pressures that pushed Ames to cooperate with the KGB and become a spy in April 1985 (Senate Select Committee on Intelligence, 1994:11).

Ames' emotional state while evaluating his options clearly played a role. There is, however, another point to consider. Ames has stated that committing espionage came very easily to him (Earley, 1997:136). He explains that there should have been 'barriers' preventing him from going forward with his plan to betray his country (Earley, 1997:145-146). His judgement, however, was somehow impaired, and he was able to rationalise his actions. He states that in the end 'there was only one barrier left, and that was one of personal loyalty to the people [he] knew and, unfortunately it was not a very strong one' (Earley, 1997:145-146).

There were also other factors that most likely affected Aldrich Ames' judgement. He had a history of problematic behaviours related to his excessive consumption of alcohol, such as the following:

- Repeatedly violating DUI laws (Senate Select Committee on Intelligence, 1994:5);
- Being arrested for reckless endangerment (Senate Select Committee on Intelligence, 1994:5);
- Causing an automobile accident while severely intoxicated (Senate Select Committee on Intelligence, 1994:8);

- Causing embarrassment to his first and second wife because of his alcohol-induced behaviour at social events (Earley, 1997:54 & 112-113);
- Causing embarrassment to the U.S. embassy in Mexico because of an altercation he had with a Cuban official during an official diplomatic event (Senate Select Committee on Intelligence, 1994:8); and
- Becoming so intoxicated during lunch breaks at least once per week that he would be unable to work in the afternoon (Senate Select Committee on Intelligence, 1994:24).

These events bring into question whether Ames' judgment was also in some way affected through his excessive alcohol consumption while deciding how best to address his problems. Moreover, it also seems noteworthy that Ames himself observes that while looking for solutions to his problems, he only considered options that were illegal (Earley, 1997:136). This, combined with several other observations seem to be consistent with an antisocial personality disorder. This would be an important finding because the antisocial personality disorder is associated with an increased 'likelihood of unreliable behavior, poor judgment, and compromised motivation' and, therefore, poses a level of security risk (Shechter & Lang, 2011:vii & 2). According to DSM-V, individuals with this disorder meet three or more of the following criteria:

- 'Failure to conform to social norms with respect to lawful behaviors, as indicated by repeatedly performing acts that are grounds for arrest.
- Deceitfulness, as indicated by repeatedly lying, use of aliases, or conning others for personal profit or pleasure.
- Impulsivity or failure to plan ahead.
- Irritability and aggressiveness, as indicated by repeated physical fights or assaults.
- Reckless disregard for safety of self or others.
- Consistent irresponsibility, as indicated by repeated failure to sustain consistent work behavior or honor financial obligations.
- Lack of remorse as indicated by being indifferent to or rationalizing having hurt, mistreated, or stolen from another' (American Psychiatric Association, 2013:659).

Apart from his espionage-related arrest, Ames was arrested three times for alcohol-related violations and once for speeding and reckless driving (Earley, 1997:37; Senate Select Committee on Intelligence, 1994:5). Ames repeatedly failed to sustain consistent work behaviour by breaching security protocol (e.g. forgetting classified documentation and identity cards, or accidently leaving them behind at a ballpark and on a subway, thereby leaving himself and his assets exposed) (Senate Select Committee on Intelligence, 1994:5, 7 & 10). His overall work performance was also a point of concern. He was known for procrastinating in his work, failing to file his official financial accountings; failure to close out his personal financial accounts upon leaving a duty station; and late in reporting his sanctioned meetings with Soviet officials and his romance with Rosario (Senate Select Committee on Intelligence, 1994:24). Finally, Ames offered several rationalisations with which he sought to justify his acts of espionage (Earley, 1997:145-146).

Ames decided that espionage would be the best option to solve his problems. On 16 April 1985, Ames entered the Soviet Embassy in Washington D.C. He handed an envelope to the duty officer that was addressed to Sergey Dimitriyevich Chuvakhin, the most senior KGB officer at the embassy. Ames had the opportunity to have a brief conversation with Chuvakhin before leaving the embassy (Senate Select Committee on Intelligence, 1994:12). This was the beginning of a sequence of events which culminated in Ames' recruitment as a spy and receiving his first payment ($50,000 in cash) in May 1985. His career as a Soviet spy continued for nine years and brought him an income of $2.5 million (Senate Select Committee on Intelligence, 1994:2). His marriage with Rosario lasted until their arrest. In exchange, Aldrich Ames provided his handlers a trove of classified documents and the names of twenty CIA assets in Russia, six of whom were subsequently executed (Senate Select Committee on Intelligence, 1994:14-15 & 143-144).

5.4 INSIDER ESPIONAGE AS AN ICT-SUPPORTED COMMERCIAL ENTERPRISE: THE BRIAN REGAN CASE

Brian Patrick Regan was a U.S. Air Force non-commissioned officer who later became a defence contractor from 1980 until the time of his arrest on grounds of espionage in 2003 (Bhattacharjee, 2016:8 & 89). Regan downloaded and printed out approximately 20,000 pages of classified documentation from Intelink which he intended to sell to foreign adversaries of the United States. Intelink is the intranet of the U.S. intelligence community and a vital tool enabling members of the U.S. intelligence agencies to share and disseminate a vast amount of classified information. The information that Regan collected included intelligence reports by American spies across the world, image analyses and signals collected through reconnaissance (Bhattacharjee, 2016:102). The case of Brian Regan is an interesting one because it was the first known instance of insider espionage in which vast amounts of data were stolen using modern ICT technologies. While the full scope of his espionage activities remained unclear, it is certain that he contacted and provided a sample of classified information to the Libyan government (Bhattacharjee, 2016:8). In 2003, Regan was imprisoned for life for committing espionage (Bhattacharjee, 2016:226).

5.4.1 Personal background

Brian Patrick Regan was born in New York City on October 23, 1962, as the third of eight children (Bhattacharjee, 2016:57). His parents, Michael and Anne Regan, had emigrated to the United States from Ireland in the 1950s in search of a better life. Having settled in Farmingdale, New York, Regan's father, Michael, became a worker at a local factory that manufactured twist drills (Bhattacharjee, 2016:57). Anne worked at home managing the household and raising the couple's eight children. Michael's modest wages were the family's sole source of income and so the family lived in a small house located in a blue-collar neighbourhood that was untouched by privilege. Doing much of the construction himself, Michael eventually added a second floor to the house, to accommodate the growing family. However, even with this addition, the house was still cramped for the family of ten (Bhattacharjee, 2016:58-59).

At dinner time, the children would have to eat in shifts because there was not enough room around the table. On holidays, the family would squeeze in extra chairs from around the house so that everyone could fit. During the summer months, Regan would sometimes use the garden hose to wash up outside to get ready for school because the two bathrooms in the house were in constant use by the other members of his family (Bhattacharjee, 2016:57-58).

As he became older, Regan soon learned that he and his siblings would have to compete for ‘food, space, and parental attention in a household where all three were in short supply’ (Bhattacharjee, 2016:57). Having to share his bed with one of his brothers, Regan ‘grew out his toenails so that he could use them as little daggers to make more room for himself’ (Bhattacharjee, 2016:57-58). In his early teenage years, Regan put padlocks on his closet to protect his cookies and sweets from his brothers and sisters. Regan came to realise that he had to look out for himself because nobody else would. His survival depended on him being able to outsmart those around him (Bhattacharjee, 2016:58).

Regan’s parents were devout Catholics striving to make religion an important aspect of the family's life. Every Sunday morning, the family would get dressed and pile into their station wagon to go to church. Regan was enrolled in a Catholic school in the neighbouring town. He did not take well to the school’s stern discipline and was often in trouble. It was forbidden for the children to bring playing cards or candy to school. Regan did both and in fourth grade he began selling candy to his school mates for a profit. One day that year, Regan and three of his friends were romping around at the altar of the school chapel. One of the boys knocked over a giant candlestick. It was smashed to pieces. Regan and one of the other boys were expelled. For Regan, who had not yet reached his tenth (10) birthday, this experience was both shameful and traumatic. He discovered that the world could be an ‘unkind place’ and his expulsion was proof to him ‘that society was an adversary from which no sympathy could be expected’ (Bhattacharjee, 2016:59).

Regan’s outlook on life was further hardened by his abusive father who was quick to resort to corporal punishment at the smallest of infractions. By the time Regan entered middle school, it had become evident to his teachers that Regan was a slow learner. At best, he would have been considered to be an average student. It eventually came to light that the reason for his lacking educational progress was dyslexia. Just as others afflicted with this condition, Regan had difficulty processing and remembering sequences of written characters. It was because of this that Regan found it difficult to read and write. Similar to many other dyslexics, he also found it difficult to learn maths (Bhattacharjee, 2016:60-61). Having dyslexia does not imply low intelligence. Nevertheless, children with dyslexia are often perceived by peers, teachers and parents as being intellectually challenged. When Regan went to schoolteachers and school administrators were comparatively uninformed with respect to the special needs of dyslexic children and, therefore, provided little targeted help to Regan and other students in his situation to overcome the specific challenges they faced (Bhattacharjee, 2016:60-61).

Having dyslexia did not only adversely affect Regan’s academic performance. It also destroyed his social standing. His disability induced a permanent sense of being marginalised as an outsider. Other children with dyslexia might be able to overcome the attacks on their self-esteem by excelling in some extracurricular activity such as sports. Others can cope because they have exceptional support from their parents. Regan, however, had neither, making him an easy target of bullies in his neighbourhood. The challenges he faced with dyslexia combined with the ostracism among his peers that resulted from it contributed to Regan’s social awkwardness. ‘His affectations, his speech, and the jokes he made always seemed out of step with the others, making him an easy target for mockery. He would come up with one-liners and then break into a cackling, hyena-like laugh that the other kids usually found funnier than the joke. ‘He was a little bit odd,’ recalls Cliff Wagner, who was part of his clique. “We used to laugh at him more than with him’’ (Bhattacharjee, 2016:61-62).

To earn some money while in school, Regan had an afternoon job delivering newspapers in his neighbourhood. Similar to other newspaper-carriers, Regan would load up the front basket of his bicycle with newspapers and then proceed to deliver them. The bullies of his neighbourhood would sometimes intercept Regan, throw roof shingles at him, and knock down his bicycle with all the newspapers. In the winter months, these attacks would end up with Regan slipping and falling on the ice (Bhattacharjee, 2016:62-63). Regan felt increasingly frustrated by these attacks. When he finally decided to exact revenge at his main tormentor, his efforts failed causing him to be regarded as ‘an oddball and a clown, somebody not worth taking seriously’ even more than before’ (Bhattacharjee, 2016:62-63). However, what few knew about Regan was that he also had a knack for stealth and a willingness to use it. On one occasion, for instance, Regan broke into a house in the neighbourhood and stole a set of ceramic art tools (Bhattacharjee, 2016:66 & 102).

Regan had always been of average height and build among his peers. However, at age fifteen, he hit a growth spurt and was now suddenly one of the biggest boys. He began working out at the gym, which helped him build his physique and his confidence. After years of being bullied, he had developed into a tall, strong adolescent who now had the assets with which to fight back. Although he did not pick fights, he also did not avoid them. He would use his strength to defend friends who were less powerful than he was and who were being bullied by others. This eventually changed his standing among his peers (Bhattacharjee, 2016:67-68). His newly developed size and strength brought other benefits. Regan was able to secure an afternoon job stacking tires at a store close to his father's factory. The work was physically demanding but paid much better than the newspaper delivery job did. With the money he earned, he was able to save enough to buy a ten-year old Ford Mustang Boss 302 that the previous owner had kept in great condition. 'Overnight, the car earned Regan more admiration and respect from peers than he had ever gotten' (Bhattacharjee, 2016:68).

With his poor academic performance, Regan did not have any hopes of going to college. On the other hand, he did not want to stay at home in Farmingdale and work at the factory like his father did. The only way that he could think of getting out of the environment in which he grew up and see the world was to join the military (Bhattacharjee, 2016:69).

While Regan was in his last year of school, he therefore took the Armed Services Vocational Aptitude Battery (ASVAB), which was a three hour-long multiple-choice test that the military offered to high school students. The battery measures cognitive abilities like pattern recognition and spatial perception, but also verbal ability, as well as knowledge of science, social studies, history, and other topics. The test score would determine which branch of the armed forces (Army, Navy, Air Force, Marines, or Coast Guard) the applicant could join (Bhattacharjee, 2016:69).

The minimum score for the Air Force, Marines, and Coast Guard is higher than that required for the army or Navy. Regan took the test together with his friend Gould who was a much better student. He sat behind Gould during the test and copied Gould’s answers while the test proctor was not looking. When Regan and Gould received their test scores some months later, both were among the top scorers and had qualified to join the Air Force (Bhattacharjee, 2016:69).

Regan performed so well on the test that he was able to qualify for an assignment in intelligence, which was one of the service’s most coveted career tracks. This was Regan's opportunity to leave the humiliating life that he had experienced in Farmingdale behind. Gould, on the other hand, decided not to join the military despite his high score. Some months prior to his 18th birthday and with his mother's consent, Regan enlisted in the Air Force and began his eight-week basic training course at Lackland Air Force Base in San Antonio, Texas. He was then transferred to Goodfellow Air Force Base in San Angelo, Texas where he was trained in signals intelligence and analysis. The training program was the most challenging that Regan had ever experienced, but he was determined to succeed and applied himself rigorously to overcome the impediments that his dyslexia posed. Regan successfully completed the course and upon graduation after a few months was assigned to a U.S. air station near Iraklion on the Greek island of Crete (Bhattacharjee, 2016:70).

While in Greece, Regan met his future wife, Anette Stenqvist, a young Swedish high school student who had been visiting Greece as a tourist. After Anette’s return to Sweden, Regan maintained contact with her. Regan proposed marriage to her and upon his reassignment to Kelly Air Force Base in San Antonio, Texas, Anette joined him and the two were married (Bhattacharjee, 2016:72). Two years later, the couple moved to Osan Air Base in South Korea where Regan worked with the 6903rd Electronic Security Group. He was doing well in his job and steadily moved up in rank. His challenges with dyslexia did not prevent him from advancing in his career because of his ability to recognise patterns, which was advantageous in his job. In summer 1985 Regan and Anette moved to Wheeler Air Force Base in Honolulu, Hawaii where they lived in a spacious and well-furnished apartment (Bhattacharjee, 2016:72-73). While stationed in Hawaii, they were visited by Gould, who was Regan's old friend. Gould was impressed by how well the Regans were doing and, somewhat enviously wondered whether he should have joined the military himself.

During Regan’s visits to Farmingdale, Regan’s family was equally impressed with what had become of Regan (Bhattacharjee, 2016:73). For all the challenges and blows against his self-esteem that Regan had to face in his earlier life, it appeared that he was now supported by professional success and a lifestyle that banned these memories into the distant past.

5.4.2 Triggers

Despite the successes that Regan undeniably had in his career, there are indications that his self-esteem continued to be fragile and perhaps irreparably damaged through the experiences he had early in life. From Hawaii, Regan and his family were transferred to Chantilly, Virginia where Regan was assigned to the National Reconnaissance Office (NRO). At the NRO, his work involved supporting pilot training exercises by setting up air defence systems that pilots would have to evade during simulations. Drawing on his knowledge of how countries such as Iraq and Libya deployed their radar and antiaircraft weaponry, he helped write the scripts for how the defences would work in the exercises. While this work was not without its challenges, it was a lesser task compared with the responsibilities of his colleagues who were among the brightest in the Air Force (Bhattacharjee, 2016:90 & 92).

To boost his image with others, Regan created a fake CIA placard for his car, which he made by printing out a CIA emblem and pasting it on a piece of cardboard along with the words ‘on official CIA business’. While traveling around the United States, he would place the placard under his windshield with the aim of impressing women he was hoping to meet (Bhattacharjee, 2016:94). Regan frequently had one-night stands that he organised through Craig’s List (Bhattacharjee, 2016:96). Whenever his colleagues were due to go on a business trip, he would boastfully give them the impression that he had already been at that location and that he knew the best hotels. His descriptions were not, however, based on actual experience, but on information he gleaned from the internet (Bhattacharjee, 2016:93).

Regan was in dire financial straits with unpaid balances on a dozen credit cards amounting to tens of thousands of dollars. He kept this fact from others including his wife and family for fear that he would be seen as a failure (Bhattacharjee, 2016:96 & 98). Despite his financial troubles, he was continuously ostentatious to his colleagues about the large gains he had made by investing in the stock market and he would try to advise them on which stocks to buy. His claims, however, seemed inconsistent with the rather shabby clothing he wore, the barely functioning car he drove, and his penchant for thrift (Bhattacharjee, 2016:93). He also attempted to improve his self-image and social standing by borrowing audio books from the library with which he tried to teach himself history, sociology, and other subjects. He correctly felt that his colleagues considered him unsophisticated, but he had hoped that by walking this path of self-improvement, he would be able to convince them otherwise. This was to no avail (Bhattacharjee, 2016:94).

Regan's work was quite different from that of the other colleagues in his unit. Most of them were ‘assigned to higher-order tasks that were more intellectually demanding: assessing the quality of the signals intelligence gathered, writing reports on the performance of the NRO systems, making recommendations to improve them’ (Bhattacharjee, 2016:92). During staff meetings, Regan’s presentations were often swiftly dismissed so that the group could move on to more interesting topics. Regan had fought an uphill battle to prove his intellectual capability since childhood and he was again in a situation in which he was made to feel inadequate. This sense was further exacerbated by his colleagues’ banter. They joked about his odd personality, untidy physical appearance, messy desk, and car that frequently broke down (Bhattacharjee, 2016:92).

Regan was not just isolated at work. The pressure of raising four children and Anette’s unfulfilled dreams of becoming a Hollywood actress had caused Anette to become bitter and their marriage to fray. Anette loved horseback riding, which was a considerable expense for the family and, oblivious to the gravity of the couple’s financial difficulties, she hoped to own a horse ranch someday. ‘The marriage wasn't loveless, but it was in choppy waters’ and the dream of owning a horse ranch was clearly out of step with the couple’s financial reality’ (Bhattacharjee, 2016:95).

Given his professional environment and his performance evaluations, which were average, it was evident that Regan could not expect a promotion anytime soon. The Air Force, therefore, wanted to transfer him back to Europe, but Regan was unwilling to move for fear that this would cause further disruption to his family. He asked for a deferment of the transfer, but the Air Force, offered a different alternative. If he was not willing to move, he could remain in post until he reached twenty years of service a year later and then retire. He accepted this alternative, but it further exacerbated his situation (Bhattacharjee, 2016:101).

5.4.3 Motives

Regan's situation turned into the perfect storm. He had already been faced with the constant barrage of humiliations at work, a worsening financial situation, and the growing rift in his marriage. Having been pushed by the Air Force to choose between transferring to Europe or accepting an early retirement, he grudgingly opted for the latter, which he considered to be the less disruptive for his family (Bhattacharjee, 2016:101). This choice, however, put Regan under increasing pressure. The closer he came to his unwanted retirement, the more it dawned on him that the narrow scope of responsibilities he had with the NRO might prevent him from finding a well-paying job in industry. He began to realise that he would most certainly not gain employment with the same ease that his departing NRO co-workers could expect. He was faced with increasing uncertainties regarding his future, and it appeared that there was little he could do to contain or control this situation (Bhattacharjee, 2016:101).

Regan's appraisal of his situation caused him to feel increasingly anxious. In the absence of any promising job prospects, he tried to find other ways out of his situation. He thought up various schemes to secure a brighter future such as investing in the stock market, trying his luck in gambling in Las Vegas, and marketing a baby-bottle-dryer he had invented. But all of these schemes failed and with his retirement drawing closer, he became increasingly desperate and his anxiety about the future finally developed into panic. Regan was clearly ready to act on this situation, but he had yet to decide on how (Bhattacharjee, 2016:97 & 101).

5.4.4 Situational vulnerabilities

Apart from his primary tasks, which involved supporting the scripting of air defence training exercises for pilots, Regan was also responsible for maintaining his division's Web page on Intelink. Through Intelink, Regan had access to tens of thousands of Web pages containing a wide array of secrets that had been gathered by the United States intelligence community (Bhattacharjee, 2016:97 & 102). Regan was able to explore the depth and breadth of Intelink in areas that went well beyond his responsibilities. The lack of compartmentalisation gave him access to such materials like ‘a diverse selection of images and intelligence reports, a profile of a Libyan general, the United States' capabilities for destroying military sites hidden deep underground, an adversary's handbook for conducting biological warfare’ (Bhattacharjee, 2016:103).

Regan’s surfing activities on Intelink went unchecked. He began printing out documents that were peripheral to his core assignment, but his frequent trips to the printer went unnoticed at his office. At some point, he began compiling the information from the websites using the Snagit programme, which enabled him to copy several pages into a single file. This too went undetected (Bhattacharjee, 2016:103). He repeatedly stored his printouts in a locked credenza that was located between his cubicle and that of his neighbour. This, however, also never raised any suspicion. On one occasion, while Regan was on a business trip, the NRO's facility management staff was combing the offices looking for unused furniture. They took along the credenza, drilled it open and found hundreds of printouts that Regan had concealed there. Having realised that the credenza was still being used, they contacted Regan to ask whether the documents were his. When he confirmed that they were, the facility management staff wrapped up the documents and returned them to Regan. The fact that these documents were unrelated to his work also went unnoticed (Bhattacharjee, 2016:106). Regan eventually began copying information from Intelink onto CD-ROMs which he also stashed in his office. Finally, he took video cassettes containing classified training materials home and copied them onto empty cassettes before returning them to the NRO (Bhattacharjee, 2016:106).

Both the Air Force and the NRO were evidently unaware of Regan’s financial difficulties, which might have been a red flag particularly in light of his approaching departure from the Air Force. This suggests that the personnel security measures that were in place were not rigorous enough to detect the possible vulnerability (US Government, 2017:n.p.). Moreover, Regan had complete access to the information available on Intelink up to the Top-Secret classification level. The fact that he could access information unrelated to his work suggests that there were issues related to compartmentalisation. Finally, the document storage policies evidently did not serve to prevent or detect his actions (Prunckun, 2019:131). ICT security measures *inter* alia aim to ensure that information resources contained in the system can only be accessed by individuals who are authorised to access them. While Regan's Top-Secret security clearance gave him that authorisation, it is questionable whether it also should have allowed him access to information that was unrelated to his work (Wąsiński, 2015:72).

When entering and leaving the RSO premises, all staff were required to pass through turnstiles and could be spot-checked by security guards. However, at the end of a workday, with dozens of employees leaving the building, being checked by the guards was an unlikely occurrence. The guards typically 'milled around at the front desk, chitchatting among themselves as people streamed out' thus leaving the organisation exposed in terms of physical security countermeasures as well (Bhattacharjee, 2016:107). Over several occasions, Regan was able to smuggle vast amounts of material past the guards using a sports bag. In this way, he removed more than 20,000 documents and CD-ROMs until he finally had his entire treasure trove stashed in the basement of his home (Bhattacharjee, 2016:107 & 109).

5.4.5 Market opportunities

Regan was faced with grave financial difficulties, a fraying marriage, an impending retirement from the Air Force, which he resented, and lacking career prospects for the time after his retirement (Bhattacharjee, 2016:101). In the absence of other options to remedy his situation, Regan came to see the access he had to classified information through Intelink as a source of great potential wealth. He only had to find customers - enemies of the United States - who were willing to pay (Bhattacharjee, 2016:104-105).

In April 2000, Regan started working on a plan how to market the documents that he had stolen. He could have simply walked into the Washington embassies of Iraq, Libya, Iran, and Sudan which he knew to be enemies of the United States. He was, however, also aware that these embassies were being observed by the FBI. If he had been seen entering any one of them, it could have ended his plot before it began

(Bhattacharjee, 2016:105 & 108). He, therefore, began exploring the locations of the embassies of these four countries in France, Germany, and Switzerland where he was more certain to avoid detection (United States District Court for the Eastern District of Virginia, 2001a; Bhattacharjee, 2016:126).

Regan sorted the printouts and CD-ROMs he had stolen by target country and bundled them into packages. He felt most optimistic about Libya and Iraq and focused his efforts on them first (Bhattacharjee, 2016:109-110). Furthermore, he prepared a letter to the Libyan intelligence service in which he (inaccurately) introduced himself as a CIA analyst. In this letter, he highlighted the type of secrets he was willing to provide, and he asked for $13 million in exchange. To establish *bona fides* he added a sample of the kind of secret information he had access to (United States District Court for the Eastern District of Virginia, 2001b; Bhattacharjee, 2016:108). The sample contained an array of documents classified ‘Secret’ including electronic images taken from overhead platforms, portions of a CIA intelligence report, two (2) classified pages from a CIA newsletter, and a document relating to the Libyan satellite capability (United States District Court for the Eastern District of Virginia, 2001b).

Regan posted this material to the Libyan Embassy in Washington and put the rest in Tupperware containers which he buried at seven dead drops in a nearby forest for his later transactions (Bhattacharjee, 2016:110 & 220). Regan flew to Berlin and travelled on to Munich in June 2001. According to the criminal complaint against Regan, his trip was not in connection with any of his official duties. The implication was that the purpose of the trip was to meet with embassy representatives of his target countries. It appears, however, that this could not be substantiated because it would otherwise have been stated in the criminal complaint. The criminal complaint suggests that Regan was apprehended by the FBI before an exchange of money for information could occur (United States District Court for the Eastern District of Virginia, 2001b).

5.4.6 Disinhibiting factors

The grave financial difficulties, fraying marriage, impending retirement from the Air Force, and lack of career prospects for the time after his retirement caused Regan to experience considerable anxiety (Bhattacharjee, 2016:101). Heuer (2001:n.p.), however, reminds us that there are probably many individuals in the intelligence community who would have a motive to engage in espionage, but there are few who actually do. The question, therefore, is why Regan chose to commit illegal activities. As his retirement drew closer, his anxiety grew into panic (Bhattacharjee, 2016:101).

Panic is a kind of intense fear, which motivates the individual to find some avenue of escape (Deckers, 2016:389). Regan was desperate to find a way out of his dilemma and it had become clear to him that the legal avenues (i.e. stock market investments, inventions, Las Vegas gambling, well-paying job prospect) were not going to produce the desired outcomes. In his own perception, Regan was left with one option, albeit an illegal one, and that was to steal classified documents from the government and sell them to enemies of the United States (Bhattacharjee, 2016:104-105). Having realised how easily he could steal the secret documents and having thought through the actions he could take to avoid discovery, Regan evidently concluded that the risk of detection was not as great as the risk of financial ruin (Bhattacharjee, 2016:102-103 & 105-106). He, therefore, chose the path that offered him greater certainty of a positive outcome, which was espionage. This was to become the action through which he could allay his fears (United States District Court for the Eastern District of Virginia, 2001b).

Fear, however, can alternatively lead to inaction (Deckers, 2016:389). In Regan’s case, this would have meant accepting personal bankruptcy. But he knew that his wife, Anette, would not want to face this social embarrassment (Bhattacharjee, 2016:99). Apart from his fears, which were evidently strong determinants of his actions, the fact that he lacked the inhibitions to violate legal norms may have been reinforced by a personality disorder:

- ‘Failure to conform to social norms with respect to lawful behaviors, as indicated by repeatedly performing acts that are grounds for arrest’;
- ‘Deceitfulness, as indicated by repeatedly lying, use of aliases, or conning others for personal profit or pleasure’;
- ‘Consistent irresponsibility, as indicated by repeated failure to sustain consistent work behavior or honor financial obligations’; and

- ‘Lack of remorse as indicated by being indifferent to or rationalizing having hurt, mistreated, or stolen from another’ (American Psychiatric Association, 2013:659).

As indicated in Table 3.11 of Chapter 3, these are four of the seven criteria corresponding with an antisocial personality disorder which suggests that Regan was affected by this condition (American Psychiatric Association, 2013:659). The antisocial personality disorder is one of the conditions that can pose an increased risk regarding the handling of classified information because of the ‘likelihood of unreliable behavior, poor judgment, and compromised motivation’ (Shechter & Lang, 2011:2).

There are aspects in Regan’s behaviour that appear to be consistent with these characteristics. His failure to conform with social norms is evidenced by:

- The burglary he committed as a teenager (Bhattacharjee, 2016:66 & 102);
- His cheating on the Armed Services Vocational Aptitude Battery (ASVAB) (Bhattacharjee, 2016:69); and
- His theft of government property (Bhattacharjee, 2016:106).

Deceitfulness, as indicated by repeatedly lying, use of aliases, or conning others appears evidenced by the following attributes of Regan:

- Falsely assuming the persona of a CIA on official business to impress others;
- Using this false persona to seduce women into one-night-stands (Bhattacharjee, 2016:94);
- Pretending to have stayed at the best hotels at locations that his colleagues were due to visit; and
- Making false claims about having achieved great gains in the stock market as a basis to offer his colleagues investment advice (Bhattacharjee, 2016:93).

Evidence of a lack of financial responsibility is provided through:

- Regan’s repeated gambling, which caused considerable losses;
- His repeatedly failed stock investments, which also caused considerable losses;
- His juggling of credit card debt between credit cards;
- His regular visits to expensive restaurants despite his financial problems; and

- His unwillingness to address the considerable costs associated with his wife's equestrian activities (Bhattacharjee, 2016:93 & 96).

Finally, there was no indication of remorse resulting from the theft of government documents. On the contrary, he repeatedly engaged in these acts and later put considerable effort into grouping the documents into packages according to the target countries (customers) (Bhattacharjee, 2016:109-110). Despite these efforts, the exchanges he had foreseen never occurred because he was apprehended by the FBI before he could complete his plan.

5.5 INSIDER ESPIONAGE AS A MASS DATA COLLECTION OPERATION: THE EDWARD SNOWDEN CASE

Edward Snowden is a computer expert who worked as a contractor and staff employee for the CIA and was later employed as a contractor for the National Security Agency (NSA) (United States District Court for the Eastern District of Virginia, 2019:n.p.). In 2012, while working as an NSA contractor, Snowden downloaded more than 50,000 documents related to the U.S. government's electronic spying programmes and secretly turned them over to Ewen MacAskill, Glenn Greenwald, and Laura Poitras during a clandestine meeting in Hong Kong. At the time, MacAskill was the defence and intelligence correspondent of the British newspaper, The Guardian, and Greenwald was a lawyer and a columnist for The Guardian. Poitras was a documentary film director who occasionally did pieces for The New York Times (Maass, 2013:n.p.).

After three days of interviews at a hotel in Hong Kong, Greenwald, MacAskill, and Poitras published the material they had collected. Soon after, at Snowden's request, Greenwald, MacAskill and Poitras (2013:n.p.) released the name of their source. Snowden was subsequently charged with theft of government property, unauthorised communication of national defence information, and communication of classified communications intelligence information to an unauthorised person (i.e. espionage) (United States District Court for the Eastern District of Virginia, 2013:n.p.; United States District Court for the Eastern District of Virginia, 2019:n.p.). His act of espionage is regarded as the worst breach of classified data in the 61-year history of the NSA (Hosenball & Strobel, 2013:n.p.).

5.5.1 Personal background

Edward Joseph Snowden was born in Elizabeth City, North Carolina on June 21, 1983, as the younger of two children. At the time of his birth, Snowden's father, Lon, was a chief petty officer who was working as a curriculum designer and electronics instructor at the Coast Guard's Aviation Technical Training Center in Elizabeth City. Snowden's mother, Elizabeth, was a homemaker who put considerable effort into educating her children, Jessica and Edward, by teaching them to read, frequently taking them to the library, and assigning them age-appropriate chores around the house (Snowden, 2019:21-22).

When Snowden was eight years old, he and his family relocated from North Carolina to Crofton, Maryland where both of his parents took up assignments working for the government. Both parents were required to hold a top-secret security clearance for their work. His mother was a clerk at an insurance and benefits association, which provided services to members of the NSA. The work of Regan's father was veiled in secrecy and Regan knew very little about his father's career other than that he had become a chief warrant officer in the Aeronautical Engineering Division at Coast Guard Headquarters in Washington, DC (Snowden, 2019:34 & 36-37).

For the Snowden family, moving to Crofton meant both a financial and a social improvement. They lived in a neighbourhood primarily inhabited by families associated with the diplomatic corps and the intelligence community. Snowden describes his neighbourhood as having streets that were 'tree-lined and pretty much crime-free' with a 'multicultural, multiracial, multilingual population, which reflected the diversity' of the neighbourhood's community, which was 'well-to-do and well educated' (Snowden, 2019:36).

According to his own accounts, Snowden's adolescence centred around his family's desktop computer, a Compaq Presario 425, and the coincidental exchanges he had with others when using it. What few interests he might have had in being outdoors beforehand, these were irrevocably lost through his attraction to the computer. He writes about this period: 'If previously I'd been loath to go outside and kick around a ball, now the very idea seemed ludicrous.' The computer had become his 'constant companion [his] second sibling, and first love' (Snowden, 2019:39-40). He eventually spent all of his waking hours on the computer and would even sneak to the computer at night while his parents were asleep. Snowden writes:

> From the age of twelve or so, I tried to spend my every waking moment online. Whenever I couldn’t, I was busy planning my next session. The Internet was my sanctuary; the Web became my jungle gym, my treehouse, my fortress, my classroom without walls. If it were possible, I became more sedentary. If it were possible, I became more pale. Gradually, I stopped sleeping at night and instead slept by day in school. My grades went back into free fall (Snowden, 2019:42).

At the beginning of his sophomore year, his fatigue became even more pronounced than it had been during the preceding years. After a blood sampling, his lab results revealed that he had contracted mononucleosis, a virus commonly diagnosed among teenagers and young adults. For Snowden, this illness was both debilitating and humiliating. The humiliation resulted from the notion that this illness is contracted by, in his words ‘hooking up’ with others. However, as Snowden phrases it, the only ‘hooking up’ he had done was with a modem. Snowden’s social life appears to have been nearly non-existent. His situation was further exacerbated by his illness. For months, he no longer had the energy to spend time on the computer (Snowden, 2019:64).

After four months of absence, Snowden received a letter from his high school informing him that he had to repeat his sophomore year due to his extended absence. He was aware of this inevitability, for which he had waited fearfully for weeks. He found the thought of having to repeat two semesters at school intolerable and began looking for an ‘escape’ route, a ‘hack’ as Snowden put it (Snowden, 2019:65). After some research, Snowden learned that he did not require a high school diploma to apply to the local Anne Arundel Community College (AACC). He attended classes two days a week and by taking these classes, which were above his sophomore grade level, he was no longer obligated to repeat his tenth year (Snowden, 2019:65-66).

Describing his time at AACC, Snowden remarks that the ‘anonymity of the school suited me fine, though, as did my classes, most of which were distinctly more interesting than anything I’d napped through at Arundel High’ (Snowden, 2019:66). Despite his appreciation for the classes at AACC, he had no intention of continuing with his higher education. For Snowden, attending college classes was merely a ‘hack’ to avoid having to repeat his sophomore year in high school (Snowden, 2019:65). While he had no aspirations to complete a college credential, he was determined to complete his high school education. Rather than graduating from the high school in which he was enrolled, he decided to drop out and expedite the process by taking the battery of General Education Development (GED) exams. That way, he held a credential that ‘the US government recognises as the standard equivalent to a high school diploma’. Reflecting on his GED certificate, he averred that it was ‘a hack, but it was more than that. It was me staying true to my word’ (Snowden, 2019:68). His intention, after all, was to achieve a high school credential.

While attending classes at AACC, Snowden met Mae, a fellow student, who owned a successful small business specialised in web design. Recognising his abilities on the computer, Mae hired Snowden, who was sixteen years old at the time, to work for her as a freelancer. Snowden continued working for Mae for two (2) years (Snowden, 2019:70-71). During this time, he came to understand that his GED certificate would not take him far in his career and that he would need further credentials. Responding to a commercial he heard on the radio, he decided to enrol in a programme offered by a private company that was situated on a satellite campus of the renowned Johns Hopkins University. Snowden wrote in his autobiography:

> I found myself dialling the 1-800 number and signing up for the Micro- soft certification course that was being offered by the Computer Career Institute at Johns Hopkins University. The entire operation, from its embarrassingly high cost to its location at a ‘satellite campus’ instead of at the main university, had the faint whiff of a scam, but I didn’t care. It was a nakedly transactional affair – one that would allow Microsoft to impose a tax on the massively rising demand for IT folks, HR managers to pretend that an expensive piece of paper could distinguish bona fide pros from filthy charlatans, and nobodies like me to put the magic words ‘Johns Hopkins’ on their resume and jump to the front of the hiring line (Snowden, 2019:73).

Although he was interested in the subject matter, Snowden became impatient with the course work and therefore tried, without success, to expedite his completion of the programme by taking the tests precipitately. Since the Computer Career Institute did not give refunds on failed exams, Snowden was left with considerable debt and no credential (Snowden, 2019:74). He was still working for Mae during the 9/11 attacks on the World Trade Center and the Pentagon in 2001. Appalled at what had happened, he joined the Army in 2003 and eventually began training as a Special Forces Green Beret. While training, he suffered bilateral tibial fractures which caused him to leave the military in 2004 (Snowden, 2019:84 & 88).

In 2005, Snowden was employed as a security guard for one of the NSA's covert facilities at the University of Maryland. While this was not the type of work Snowden had hoped for, it did pay the bills and, most importantly, it gave him the coveted TS/SCI (i.e. Top Secret/Sensitive Compartmented Information) security clearance (Greenwald et al., 2013:n.p.; Snowden, 2019:114). Snowden switched jobs within the year and became a systems engineer for the CIA (Snowden, 2019:2; United States District Court for the Eastern District of Virginia, 2019:5). By his own account:

> 'The agencies were breaking all of their own rules in their quest to hire technical talent. They'd normally never hire anybody without a bachelor's degree, or later at least an associate's, neither of which I had. By all rights, I should never have even been let into the building' (Snowden, 2019:2).

In 2007, the CIA stationed Snowden at the US Embassy in Geneva under diplomatic cover where his job was to bring 'the CIA into the future by bringing its European stations online, digitising and automating the network by which the US government spied' (Snowden, 2019:2). Snowden describes his work in Geneva:

> 'My generation did more than reengineer the work of intelligence; we entirely redefined what intelligence was. For us, it was not about clandestine meetings or dead drops, but about data' (Snowden, 2019:2).

In 2009, Snowden returned to the United States, left the CIA, and joined Dell as a contractor working for the NSA. In this capacity, he was sent to Japan. He described his assignment:

> I helped to design what amounted to the agency's global backup – a massive covert network that ensured that even if the NSA's headquarters was reduced to ash in a nuclear blast, no data would ever be lost. At the time, I didn't realize that engineering a system that would keep a permanent record of everyone's life was a tragic mistake (Snowden, 2019:2-3).

Snowden returned to the United States in 2011 and received a promotion which put him in charge of the technical liaison team handling Dell's relationship with the CIA. In this role, he met with the heads of the CIA's technical divisions 'to design and sell the solution to any problem that they could imagine including the introduction of a ‘cloud’ which would enable intelligence officers, regardless of where they were physically located, to access and search any data they needed, no matter the distance’ (Snowden, 2019:2-3).

After four (4) years with Dell, Snowden applied for a job with Booz Allen Hamilton where he would continue working for the NSA. It later came to light that he embellished his educational profile in the resumé he submitted. He stated that he had taken computer- related classes at Johns Hopkins University, a Tokyo campus of the University of Maryland, and the University of Liverpool in Britain and that he was expecting to receive a master’s degree in computer security from University of Liverpool later that year. Booz Allen Hamilton subsequently hired Snowden as a contractor for the NSA in Hawaii (Hosenball, 2013:n.p.; Snowden, 2019:72).

The statements in Snowden’s resumé regarding his studies at the University of Maryland and the University of Liverpool were misleading. According to a spokesperson of the University of Maryland, Snowden had only attended a summer session at the university’s campus in Asia and according to a University of Liverpool spokesperson, ‘Snowden had registered for an online master’s program in computer security in 2011’. But the spokesperson added that “he [was] not active in his studies and has not completed the program” (Hosenball, 2013:n.p.). To enter the University of Liverpool’s MSc in Cyber Security programme, applicants must either possess ‘A degree in computer science or a closely related subject, equivalent to a UK bachelor’s degree, coupled with two years’ relevant IT professional experience; or have gained professional work experience in IT or a related field and/ or other prior qualifications, which are considered on a ‘case-by-case basis’ (University of Liverpool, 2022:n.p.).

Given Snowden’s academic background, his enrolment at the University of Liverpool would most certainly have been based on the IT experience he acquired rather than a completed degree in computer science. However, since entry into a master’s programme in the United States generally requires a completed bachelor’s degree (Danesy, 1994:85), recruiters in the United States would certainly have taken Snowden’s enrolment in the master’s programme at the University of Liverpool to mean that he had completed a bachelor’s degree.

A month into his contract with Booz Allen Hamilton, Snowden informed his NSA supervisor that he would have ‘to be away from work for a couple of weeks in order to receive treatment for epilepsy, a condition he learned he suffers from after a series of seizures’ the previous year (Greenwald et al., 2013:n.p.). Rather than to tend to his medical condition, however, the purpose of his absence was to travel to Hong Kong where he was planning to meet with journalists to disclose his countries' secrets. He chose Hong Kong because he associated it with ‘a spirited commitment to free speech and the right of political dissent’ and because he believed that the city would resist any extradition requests from the United States (Greenwald et al., 2013:n.p.).

5.5.2 Triggers

Growing up, Snowden became acutely aware of the role his ancestors played in the history of the United States. The European colonisation of Maryland began in 1634. Twenty-four years later, in 1658, the English army sent a Major Richard Snowden to Baltimore where he was to protect the interests of the Crown. Meanwhile, his brother, John Snowden, an ancestor of Edward Snowden, had been imprisoned in Yorkshire, England for preaching the Quaker faith, which was a violation against the Church of England (Snowden, 2019:33). Baltimore had passed the Maryland Toleration Act, which guaranteed religious tolerance for Trinitarian Christians including Quakers (Maryland State Archives, 2022:n.p.). In 1682, John Snowden was able to reduce his prison sentence on the condition that he would leave England and move to Baltimore (Snowden, 2019:33).

Although Quakers are characteristically pacifists, three of John Snowden's grandsons served in the Continental Army during the Revolutionary War. Despite the community censure that participation in the war would attract, they chose to fight for independence and the values of liberty and justice for which the US Declaration of Independence and Constitution have since stood. One of John Snowden's grandsons, William Snowden, a direct paternal ancestor of Edward Snowden, was imprisoned by the British and subsequently died at one of the notorious sugar house prisons in Manhattan (Snowden, 2019:33-34). Many of William Snowden's descendants served their country and this instilled a sense of obligation and commitment in Edward Snowden. He writes:

> I believe in public service – my whole family, my whole family line for centuries, is filled with men and women who have spent their lives serving this country and its citizens. I had sworn an oath of service not to an agency, nor even a government, but to the public, in support and defense of the Constitution (Snowden, 2019:6).

This is an important facet in the Snowden case, because, in his understanding, the United Sates government was violating constitutional rights. Above all, there were two events that triggered Snowden's acts of espionage. The first event was the NSA's construction of a vast new twenty-five-thousand-square-foot data facility, the Mission Data Repository (MDR) which, in Snowden's words, would 'hold an immense amount of data, basically a rolling history of the entire planet's pattern of life, insofar as life can be understood through the connection of payments to people, people to phones, phones to calls, calls to networks, and the synoptic array of Internet activity moving along those networks' lines' (Snowden, 2019:246). In Snowden's view, there was no good reason to build a facility with these specifications unless 'you were planning on storing absolutely everything, forever'. He regarded the MDR as 'the corpus delicti – the plain-as-day corroboration of a crime, in a gigantic concrete bunker surrounded by barbed wire and guard towers, sucking up a city's worth of electricity from its own power grid in the middle of the Utah desert' (Snowden, 2019:247).

The second event occurred a year later. James Clapper, who was the Director of National Intelligence at the time, was required to testify before the US Senate Select Committee on Intelligence amidst concerns that the NSA was engaged in bulk collection of the communications of American citizens. In response to the question whether the NSA was collecting 'any type of data at all on millions or hundreds of millions of Americans' Clapper replied, 'No, sir … Not wittingly. There are cases where they could inadvertently perhaps collect, but not wittingly' (Wyden, 2013:6:50-7:06).

5.5.3 Motives

According to Snowden's appraisal, the testimony under oath by James Clapper, the Director of National Intelligence, before the US Senate Select Committee on Intelligence was a 'bald-faced lie, of course, not just to Congress but to the American people. More than a few of the congress people to whom Clapper was testifying knew very well that what he was saying was untrue, yet they refused, or felt legally powerless, to call him out on it' (Snowden, 2019:231 & 247). Snowden regarded the bulk collection of the American citizens' communications as a blatant transgression of their constitutional rights. He was certain that this encroached on the liberties of American citizens. To that effect, Snowden reflected that 'a government may not infringe into that domain of personal or individual freedoms that during the American Revolution was called 'liberty' and during the Internet Revolution is called 'privacy'' (Snowden, 2019:7). In his view, the leaders of the US intelligence community were responsible for this violation in which the government was complicit. With Barack Obama as president, Snowden hoped that the intelligence community would be held accountable by the Supreme Court or Congress, but this was not the case in his view (Snowden, 2019:232-2333).

By his own account, these events caused Snowden to feel lost, to fall into a dark mood, and to struggle with his conscience. His love for his country, his belief in public service, and his commitment to the Constitution and civil liberties now stood in opposition to the government's actions. He felt that his core values had been 'flagrantly violated' (Snowden, 2019:6). What made matters worse for him was that he was more than just a part of that violation by association, he 'was party to it' through his work. He was guilt-ridden and questioned how he could balance his 'contract of secrecy with the agencies that employed [him] and the oath [he had] sworn to [his] country's founding principles' (Snowden, 2019:6).

In Snowden's view, the violations against the personal liberties of the American people were intolerable. He felt that something had to be done to bring about a change. In the absence of adequate actions by the executive or the legislative branch of the government, it would have to be up to the 'Fourth Estate' (i.e. the press) to intervene (Snowden, 2019:245-246). This, however, gave rise to Snowden's next problem: 'I knew at least two things about the denizens of the Fourth Estate: they competed for scoops, and they knew very little about technology. It was this lack of expertise or even interest in tech that largely caused journalists to miss two events that stunned me while I was gathering fact about mass surveillance' (Snowden, 2019:246). Snowden thus decided to take things into his own hands. At this point, he was ready to act.

5.5.4 Situational vulnerabilities

With an IQ of 145, Snowden was a highly intelligent and articulate high school dropout who, despite not having any academic credentials, was able to manoeuvre his way into a variety of jobs with the CIA, NSA, and contractor companies working for these agencies that normally would have required not less than a bachelor's degree (Bamford, 2014:n.p.; Hosenball, 2013:n.p.; Snowden, 2019:2). A careful review of his resumé might have unveiled inaccuracies in the way that he presented his academic history. Recruiters would normally recognise such inaccuracies and regard them as warning signs if they appear to be deliberately misleading or untruthful (Heneman et al., 2019:381-382). The only evidence that the inaccuracies in Snowden's resumés were ever noticed relates to his employment by Booz Allen Hamilton. While the company noted that some of the educational information in his resumé 'did not check out', this did not prevent Booz Allen Hamilton from hiring him as a contractor for the NSA in Hawaii at an annual salary of $122,000 (Hosenball, 2013:n.p.). By his own estimation, these employers never should have hired him. But they were 'breaking all of their own rules in their quest to hire technical talent'. Normally, they would never have hired someone into these positions without at least a bachelor's degree. But astute as Snowden was in finding 'hacks', he recognised the vulnerabilities of these organisations and was able to exploit them (Snowden, 2019:2).

It was during his employment with Dell that Snowden began stealing information from the NSA. In his earlier roles as an IT specialist, Snowden had considerable access to some of the most sensitive information of the United States. But there were limits: He was 'laboring under the doctrine of 'Need to Know', unable to understand the cumulative purpose behind [his] specialised, compartmentalised tasks' (Snowden, 2019:3). When he began working for the NSA under a Dell contract in Hawaii, all that changed and he was 'finally in a position to see how all [his] work fit together, meshing like the gears of a giant machine to form a system of global mass surveillance (Snowden, 2019:3). This, however, did not prevent Snowden from wanting to gain even wider access to classified information and to conceal his effort in doing so. Snowden may have persuaded as many as 25 of his co-workers in Hawaii to give him their logins and passwords by telling them he needed them to do his job. At the time, this revelation was merely the latest to indicate ‘that inadequate security measures at the NSA played a significant role in the worst breach of classified data in the super-secret eavesdropping agency’s 61-year history’ (Hosenball & Strobel, 2013:n.p.).

To smuggle the stolen information from NSA premises, Snowden used mini- and micro-SD cards – the type one would use for digital and video cameras and for additional storage on tablets. At 20 x 21.5 mm for the mini-SD, 15 x 11 mm for the micro-SD, these storage devices proved to be ‘eminently concealable’. They could be hidden inside a pried-off square of a Rubik’s Cube, after which one would stick the square back on. He would sometimes carry the SD-card in his sock, or when feeling ‘paranoid’, in his cheek, ready to swallow it if necessary. Once he gained more confidence in smuggling the SD-cards from the NSA premises, he would simply carry the cards at the bottom of his pockets. He explained that ‘The cards sometimes triggered metal detectors, [but] the guards could always understand that someone would forget something as small as an SD-card in one’s pocket’ (Snowden, 2019:259).

While the SD-cards were optimal for the purpose of smuggling information out of the NSA premises, the amount of time required to transfer large amounts of data onto the cards was clearly suboptimal. Snowden describes the associated challenges:

> Copying times for massive volumes of data are always long-at least always longer than you want-but the duration tends to stretch even more when you’re copying not to a speedy hard drive but to a minuscule silicon wafer embedded in plastic. Also, I wasn’t just copying. I was duplicating, compressing, encrypting, none of which processes could be accomplished simultaneously with any other [storage device]. I was using all the skills I’d ever acquired in my storage work, because that’s what I was doing, essentially. I was storing the NSA’s storage, making an off-site backup of evidence of the IC’s abuses.
>
> It could take eight hours or more - entire shifts - to fill a card. And though I switched to working nights again, those hours were terrifying. There was the old computer chugging, monitor off, with all but one fluorescent ceiling panel dimmed to save energy in the after-hours. And there I was, turning the monitor back on every once in a while, to check the rate of progress and cringing. You know the feeling-the sheer hell of following the completion bar as it indicates 84 percent completed, 85 percent completed ... 1:58:53 left ... As it filled toward the sweet relief of 100 percent, all files copied, I'd be sweating, seeing shadows and hearing foot-steps around every corner (Snowden, 2019:259).

The exact number of documents that Edward Snowden removed from the NSA premises is unknown. According to an NSA security audit that was conducted after his public disclosures, it appears that he may have stolen as many as 1.7 million documents (Bamford, 2014:n.p.). His disclosures did not only implicate the NSA. The security services of Australia (ASD), the United Kingdom (GCHQ), Canada (CSEC), and New Zealand (GCSB) were also involved (Borger, 2013:n.p.; Greenwald & Gallagher, 2014:n.p.; Keck, 2014:n.p.; Leslie & Corcoran, 2013:n.p.; Weston, 2013:n.p.).

5.5.5 Market opportunities

Edward Snowden had convinced himself that the public should learn about the bulk information gathering that was being performed by the US intelligence agencies. His problem, however, was that he doubted that members of the press would have the level of technical understanding necessary to appreciate the implications of the government's activities. In his view, through the insider knowledge he had gathered and the technical expertise he possessed, he was uniquely equipped to ensure that the public would be properly informed. For a brief while, Snowden considered self-publication. This would have been the most convenient approach because he only would have had to collect the documents, communicate his concerns, post them online, and distribute the links (Snowden, 2019:240 & 243). He eventually abandoned this idea, however, because he had concerns related to authentication:

> Scores of people post 'classified secrets' to the Internet every day- many of them about time-travel technologies and aliens. I didn't want my own revelations, which were incredible already, to get lumped in with the outlandish and lost among the crazy (Snowden, 2019:243).

Snowden wanted his disclosures to be taken seriously and he feared that self-publication would undermine this objective (Snowden, 2019:243). Despite his concerns regarding the ability of journalists to understand the technical intricacies, Snowden saw no other alternative but to turn to the press. He concluded:

> … for my disclosures to be effective, I had to do more than just hand some journalists some documents - more, even, than help them interpret the documents. I had to become their partner, to provide the technological training and tools to help them do their reporting accurately and safely (Snowden, 2019:249).

Snowden considered Wikileaks which had been the ‘whistle-blower’s forum of choice’. He was attracted by the fact that Wikileaks was ‘radically skeptical’ of state power’ and ‘regularly joined up with leading international publications like the Guardian, the New York Times, Der Spiegel, Le Monde, and El Pais to publish the documents provided by its sources’ (Snowden, 2019:245). However, Wikileaks had come under considerable criticism for redacting material provided by US Army private and whistle-blower Chelsea Manning some years prior. Wikileaks had subsequently changed its publication policy and was now uploading unfiltered material into the web. In Snowden’s view, this policy would have caused the same problems of authentication that he associated with self-publication. He, therefore, dismissed the idea of partnering with Wikileaks (Snowden, 2019:245). Snowden considered contacting the New York Times as ‘America’s newspaper of record’. But recalling an incident a decade sooner in which the newspaper had – under pressure of the US government - delayed the disclosures related to STELLERWIND, the NSA’s original post-9/11 surveillance programme, by a year, Snowden hesitated to partner directly with the New York Times (Snowden, 2019:245).

Using a variety of aliases such as ‘Cincinnatus’, ‘Citizenfour’, and ‘Verax’ and offering information about the government activities, Snowden tried to establish contact with several reputable journalists. His efforts failed until he was finally able to attract the interest of Laura Poitras and Glenn Greenwald (Snowden, 2019:250-251). Poitras was a documentary film director who occasionally did pieces for The New York Times. According to Snowden, Poitras ‘had been frequently harassed by the government because of her work, repeatedly detained and interrogated by border agents whenever she travelled in or out of the country’ (Snowden, 2019:250). Greenwald had been a civil liberties lawyer who later became a columnist for Salon and eventually for the US edition of the Guardian (Snowden, 2019:250). Having learned of Snowden’s intention to provide secret information, the Guardian had Ewen MacAskill, who was a seasoned journalist, join Poitras and Greenwald in their subsequent meetings with Snowden (Greenwald et al., 2013:n.p.; Maass, 2013:n.p.; Snowden, 2019:250). In exchange for the public platform that Snowden wanted, Snowden provided the journalists with thousands and possibly hundreds of thousands of top-secret documents (Hosenball, 2013:n.p.; Maass, 2013:n.p.).

5.5.6 Disinhibiting factors

Edward Snowden grew up placing a considerable value on the US Constitution. He defined himself and his responsibilities in terms of his family history predating the US Revolutionary War. In his perception, the US Constitution was something that his 'whole family line' had defended for centuries and in his view, the US intelligence community was violating the principles of the Constitution, which he held dear (Snowden, 2019:6). The American journalist James Bamford (2014), who interviewed Snowden describes him as an 'idealist who - step by step over a period of years – grew disillusioned with his country and government' (Bamford, 2014:n.p.). According to Snowden:

> I think even Obama's critics were impressed and optimistic about the values that he represented …. He said that we're not going to sacrifice our rights. We're not going to change who we are just to catch some small percentage more terrorists (Bamford, 2014:n.p.).

In time, however, Snowden grew disappointed in the Obama administration. He states:

> Not only did they not fulfil those promises, but they entirely repudiated them …. They went in the other direction. What does that mean for a society, for a democracy, when the people that you elect on the basis of promises can basically suborn the will of the electorate? (Bamford, 2014:n.p.).

During his assignments in Japan and Switzerland, insights that Snowden gained into the field operations conducted by the US intelligence community caused his disenchantment (Bamford, 2014; Greenwald et al., 2013). Recalling his assignment in Geneva, Snowden stated:

> Much of what I saw in Geneva really disillusioned me about how my government functions and what its impact is in the world, … I realised that I was part of something that was doing far more harm than good (Greenwald et al., 2013:n.p.).

Evidently, Snowden felt so strongly about what he felt were wrongdoings of the US intelligence community that this 'led him to give up his future to share the truth about the US government's pursuit of a mass surveillance system' (United States District Court for the Eastern District of Virginia, 2019:16).

While his disillusionment and disappointment were evidently disinhibiting factors in his decision to disclose his nations secrets to the press and consequently also to enemies of the United States, there may have also been other factors affecting his decision process. Snowden has a history of deceitful behaviour. He *inter alia* 1) circumvented the requirements necessary to receive a high school diploma (Snowden, 2019:66-68), 2) falsely gave the impression that he had attended Johns Hopkins University (Snowden, 2019:72), 3) manoeuvred himself into positions for which he was not qualified (Snowden, 2019:2), and 4) conned his colleagues into providing him with their logins and passwords (Hosenball & Strobel, 2013:n.p.). By providing the press with massive amounts of documentation the consequences of which he – as an IT analyst - could certainly not have always assessed, Snowden was quite reckless in his actions. In terms of remorse, Snowden tellingly states:

> While I've never once regretted tugging aside the curtain and revealing my identity, I do wish I had done it with better diction and a better plan in mind for what was next (Snowden, 2019:293).

Deceitfulness, recklessness, and lack of remorse are markers of an antisocial personality disorder, which has been associated with cases of insider espionage (American Psychiatric Association, 2013:659; Shechter & Lang, 2011:vii). His behaviour and stated views appear to be consistent with this disorder.

There is, however, a further facet in the Snowden case. In all his contacts with journalists and in his autobiography, Snowden insisted that he did not want the focus of his disclosures to be on him, but rather on what he considered to be the misdeeds of the US intelligence community. He stated:

> I really want the focus to be on these documents and the debate which I hope this will trigger among citizens around the globe about what kind of world we want to live in (Greenwald et al., 2013:n.p.).

Nevertheless, just days after his first disclosures were published by the group of journalists, Snowden opted to forego the protection of anonymity and specifically asked that his identity be revealed with the reason of wanting to offer the public full visibility. He felt that by revealing his identity, the stories published by the journalists would gain credibility (Greenwald et al., 2013:n.p.). This reasoning, however, seems flawed since the documents Snowden handed over to the journalists speak for themselves. Since then, he has frequently given speeches for honoraria of more than $10,000. According to one estimate, he collected more than $200,000 in 2018 alone. The autobiography Snowden published in 2019 as been listed as a bestseller (United States District Court for the Eastern District of Virginia, 2019:19-20). Snowden has clearly been capitalising on his notoriety, which raises the question of whether some degree of narcissism might have also been involved.

5.6 CROSS-CASE SYNTHESIS

Strauss and Corbin (1998:58) describe data analysis as a detailed examination of data that has been extracted from data sources. In this research, the data sources were mainly biographies, autobiographies, court documents, and investigative reports related to four cases of insider espionage. In Chapter 5 of this thesis, the researcher has described the cases with the intention of providing relevant, detailed, multi-perspective information related to the subjects. According to Creswell and Creswell (2018:190-192), data analysis is the process in which researchers make sense out of the data that they have collected by taking it apart and putting it back together.

To further underpin the results of the case study method, it is possible to apply the pattern-matching technique to multiple cases and to then tie together the results of the individual case analyses in a cross-case synthesis. The cross-case synthesis involves aggregating study findings across a series of individual studies with the aim of reaching conclusions about their variables (Yin, 2018:196-197). In this study, the researcher selected four cases for analysis. In the following, the data from these four cases will be presented and analysed on the basis of the theory and conceptual framework outlined in Chapter 4. Towards this end, the researcher will address the five factors that are contained in his interdisciplinary conceptual framework, consisting of triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors, which were also used as a basis for the case analyses.

5.6.1 Triggers

Triggers are events or situations that resonate with an individual’s predispositions and initiate a motivation process (Deckers, 2016:339; Keltner & Shiota, 2003:89). Predispositions include the latent needs and beliefs, values, and ideologies of the individual (Rokeach, 1968:113; Vansteenkiste et al., 2020:1). Current approaches often neglect the fact that acts of insider espionage are preceded by triggers of some sort. However, in the following, we see that triggers have played a role in prompting individuals to become insider spies in all four cases reviewed in this study.

5.6.1.1 Triggers in the Oleg Gordievsky case

Oleg Gordievsky had come to value political, cultural, and spiritual freedom, democracy, and prosperity (Gordievsky, 2018:11). The treatment of Jews in the Soviet Union under Stalin, the Soviet suppression of the Hungarian Uprising, the building of the Berlin Wall, and the Soviet suppression of the Prague Spring were all events that conflicted with these values. While the first three triggers contributed to Gordievsky's increasing opposition to the Soviet State, it was the Soviet invasion of Czechoslovakia that gave Gordievsky the final push (Gordievsky, 2018:81-82, 98-99, 132, 213).

5.6.1.2 Triggers in the Aldrich Ames case

Before engaging in espionage, Aldrich Ames was stretched to a breaking point by conflicting obligations. Two of his needs, affiliation, and security (i.e. financial security), were seriously threatened. Ames was in a new relationship that meant very much to him and that he did not want to jeopardise. His drinking habits were, however, putting an unbearable strain on the relationship. In Ames' case, these were the circumstances that triggered his motivation process (Earley, 1997:25 & 113).

5.6.1.3 Triggers in the Brian Regan case

Brian Regan struggled with issues of lacking self-esteem which he sought to compensate by boosting his image through a variety of false representations. These efforts, however, often missed their mark. Among his colleagues he was often the subject of ridicule. His finances were in disarray and his marriage had begun to fray (Bhattacharjee, 2016:90 & 92-93). All this put Regan under considerable strain. The final push came when the Air Force presented him with the ultimatum to accept a transfer back to Europe, which he rejected, or an early retirement, which he grudgingly accepted. As his departure from the Air Force drew closer, Regan found himself without any prospects of a sustaining income after his retirement. This was the trigger for his motivation process (Bhattacharjee, 2016:101).

5.6.1.4 Triggers in the Edward Snowden case

Edward Snowden came from a long line of men and women who served the United States dating back to the American Revolutionary War. Snowden felt deeply committed to the values espoused by the US Constitution, particularly with respect to liberty and justice. Through his work with the CIA and NSA, he became aware of operations which, in his view, violated these values. He found this situation intolerable and had no hope that the US government or the press would bring about the changes he considered necessary for his country to be aligned with the Constitution. His further actions were finally triggered when the NSA began a programme of collecting bulk communications of American citizens, and James Clapper (Director of National Intelligence at the time), denied the existence of this programme under oath during a testimony before the US Senate Select Committee on Intelligence (Snowden, 2019:231 & 246-247).

There were triggers in all four cases. In Gordievsky's case the trigger was the value that he placed on freedom and democracy and his realisation through several events that the Soviet system profoundly violated these values. In Ames' case, it was the threat of his second wife leaving him (loss of companionship) and the risk of him facing financial hardship (loss of financial security). As in Ames' case, Regan was fearful of financial ruin. Moreover, his need for self-esteem, which, in any case, was already compromised and his need for belonginess in a marriage that was falling apart made him vulnerable. His undesired forced retirement from the military exacerbated his situation and became his trigger. Snowden valued liberty and justice as espoused by the US Constitution, and he felt that the US intelligence community was violating these values. His acts of espionage were triggered when the government began a program of bulk information gathering and publicly denied the existence of the programme.

5.6.2 Motives

Motivation processes are elicited by events or situations that resonate with an individual's predispositions. It is through the motivation process that motives are generated, and action readiness occurs. Motives are latent needs, beliefs, values, or ideologies that are triggered through events or situations and determine behaviour after a process of appraisal, emotional reaction, and action readiness (Deckers, 2016:369-370; Maslow, 1970/1987:60-63). We see motivation processes and the development of motives to commit espionage in all four cases reviewed in this study.

5.6.2.1 Motives in the Oleg Gordievsky case

Oleg Gordievsky witnessed the mistreatment of Jews in the Soviet Union, the suppression of the Hungarian uprising, the building of the Berlin Wall, and the invasion of Czechoslovakia during the Prague Spring. These events had a profoundly negative impact on Gordievsky. His disdain for the Soviet state grew stronger with each event. The heavy-handed Soviet operations during the Prague Spring triggered Gordievsky's motivation process. It was after this that Gordievsky could no longer contain his fury and hatred (Gordievsky, 2018:213). It was from that point onward, that he seriously began thinking about ways in which he could fight the Soviet state and it was this sentiment which motivated his further decision and actions (Gordievsky, 2018:214).

5.6.2.2 Motives in the Aldrich Ames case

Aldrich Ames saw that his drinking habits were putting a considerable strain on his relationship with Rosario, and this put him under considerable pressure. He was afraid of losing her and decided that he would have to do something to prevent this from happening. He began reflecting on different courses of action to prevent the negative outcome he feared would occur if he did not in some way become active. He was convinced that by improving his financial situation he would be able to prevent the worst from happening and this became his motive (Earley, 1997:25 & 113).

5.6.2.3 Motives in the Brian Regan case

Brian Regan's motivation process was triggered by events that jeopardised his financial security, self-esteem, and need for belongingness. He stood to suffer severe losses on all three counts, and this caused a great deal of anxiety. As his retirement drew closer and in the absence of a promising financial outlook, his anxiety developed into panic. He was intent on finding a way out of his situation (action readiness). Regan was motivated by the notion that by substantially increasing his income he would be able to improve his situation considerably. (Bhattacharjee, 2016:97 & 101).

5.6.2.4 Motives in the Edward Snowden case

Edward Snowden's actions were triggered by the NSA's programme of collecting bulk communications of American citizens and the public denial of the existence of this programme (Snowden, 2019:231 & 246-247). In his view, the values of the Constitution had been 'flagrantly violated' (Snowden, 2019:6). He was disgusted by the actions of the government and by what it meant for the American people. He felt that something had to be done to bring about a change. Snowden was motivated by the idea that the actions of his government could be stopped if they were to be exposed (Snowden, 2019:245-246). While Snowden always insisted that the purpose of his action was to expose the government and thereby thwart his government's actions, there is also evidence suggesting that Snowden had a financial motive. After his disclosures to the public, he insisted that the journalists dealing with his story make his name public. He has since become a public speaker, which has brought him honoraria of more than $10,000 per talk. According to one estimate, he collected more than $200,000 in 2018 alone. Moreover, he published his autobiography in 2019, which has been listed as a bestseller (United States District Court for the Eastern District of Virginia, 2019:19-20).

In all four cases, there were triggers, that led to appraisals that induced emotional reactions and ultimately action readiness. Gordievsky responded with fury and hatred, Ames and Regan responded to the trigger with fear, and Snowden reacted with disgust. In all four cases, the triggers combined with the appraisals and the emotional reactions motivated the individuals to remedy the issues. They were ready to act.

5.6.3 Situational vulnerabilities

Situational vulnerabilities are weaknesses in a security system, security procedure, or implementation that can be exploited (National Institute of Standards and Technology, 2021:n.p.). In a well-functioning security system, vulnerabilities are reduced through countermeasures. Countermeasures are the controls used to protect an organisation's secret information through activities that relate to 1) personnel, 2) physical layout, 3) handling of information, and 4) the cyber system and communications setup (Mehan, 2016:102; Prunckun, 2019:vii). In all four cases that have been analysed in this study, there were situational vulnerabilities that allowed the individuals to engage in espionage.

5.6.3.1 Situational Vulnerabilities in the Oleg Gordievsky case

Through his work, Oleg Gordievsky had access to top secret documents in the form of hardcopy and microfiche films. While he was not allowed to remove the hardcopies from the area in which they were stored, he did have free reign with respect to the vast number of documents he could access, and he was permitted to take notes. While this security arrangement limited the amount of information he could appropriate, it still left him with enough opportunity to selectively collect valuable secrets that he could later pass on to his handler. In comparison, the KGB was more exposed with respect to its microfiche films. Gordievsky could freely handle the films in his care. Spot-checks of offices, bags, pockets, and other items or facilities were allowed but practically never exercised. This gave Gordievsky the opportunity to leave the KGB premises with the microfiche films during his lunch breaks, have his handler copy them, and then return them unnoticed (Gordievsky, 2018:196 & 256-257).

5.6.3.2 Situational vulnerabilities in the Aldrich Ames case

In the case of Aldrich Ames, there were several ways in which the CIA was vulnerable: There was little control over the copies of documents with which Ames was able to leave the CIA premises. Spot-checks of the bags carried in and out of the premises by CIA employees were briefly introduced and then abandoned because they were considered to be inconvenient. Copies of documents were not under any system of accountability and could be carried from the premises without anyone noticing (Senate Select Committee on Intelligence, 1994:69). Similarly, at the time of Ames' espionage activity, it was possible to access documents on computers and to download them onto floppy disks without detection (Senate Select Committee on Intelligence, 1994:69). Ames could enter the offices of his colleagues and could study material 'which he had no business seeing' (Senate Select

Committee on Intelligence, 1994:69). Finally, Ames' issues with excessive alcohol consumption and associated reckless behaviour was known to his supervisors but was never further explored (Senate Select Committee on Intelligence, 1994:8). He did have at least one polygraph test after becoming a Russian spy, but despite failing the test, the examiner allowed him to pass: the reasons Ames gave for the failure of the test were accepted by the examiner at face value. The issue was never further addressed or resolved (Senate Select Committee on Intelligence, 1994:20-21).

5.6.3.3 Situational vulnerabilities in the Brian Regan case

Brian Regan was responsible for maintaining his division's Web page on Intelink. This gave him full access not only to his division's Web page, but to tens of thousands of other Web pages containing a wide array of secrets that had been gathered by the United States intelligence community. Regan was able to explore the depth and breadth of Intelink in areas that went well beyond his responsibilities. There was no compartmentalisation of the information he could access and his surfing activities on Intelink went unnoticed. He frequently printed out the web pages containing classified information and later took to copying them onto CD-ROMs. Finally, he also took video cassettes containing classified training materials home and copied them onto other cassettes before returning them to the NRO. This, too, went unnoticed (Bhattacharjee, 2016:97 & 102-103). While removing the printouts, CD-ROMs, and video cassettes from the NRO premises, Regan was required to pass through turnstiles and could have been spot-checked by security guards. In practice, however, particularly at the end of a working day, the guards rarely did any spot-checks (Bhattacharjee, 2016:107). Finally, given the level of Regan's security clearance, his financial situation, which was known to be problematic, should probably have been a red flag. This, however, does not appear to have been subject to scrutiny. This possible vulnerability also went undetected.

5.6.3.4 Situational vulnerabilities in the Edward Snowden case

Edward Snowden was able to manoeuvre his way into jobs for which he lacked the required credentials by providing inaccurate information in his resumés. Had his applications been carefully screened and assessed, these inaccuracies would most certainly have come to light, and he would not have been employed by the CIA or

NSA (Snowden, 2019:2). It only appears to have been with his last employer, Booz Allen Hamilton, where some of the discrepancies in his application were discovered. The company, however, did not pursue the matter and, instead, hired him at an annual salary of $122,000 (Hosenball, 2013:n.p.). As a systems administrator with a top-secret security clearance, Edward Snowden had considerable access to information contained in the intelligence community's computer network. He was able to gain additional access to information by persuading his co-workers, under a false pretext, to give him their login user names and passwords (Hosenball & Strobel, 2013:n.p.; Snowden, 2019:3). Snowden downloaded hundreds of thousands of classified documents onto SD-cards which he was able to smuggle past the security guards and out of the NSA premises. The SD-cards were so small that they rarely registered with the metal detectors. The guards were permitted to conduct spot checks, but rarely did (Snowden, 2019:259).

In all four cases, there were several vulnerabilities that the insider spies recognised and were therefore able to exploit. These vulnerabilities existed either because the necessary security measures did not exist or because they were not adequately applied. This made it possible for the insider spies to find a way through their respective organisation's security maze, which allowed them to extract the information.

In such a context, it is also interesting to take note of the considerable impact that developments in information technology have had over time. Oleg Gordievsky managed to provide his handlers with a comparatively modest number of documents contained in microfiche films. From one case to the next, the amount of documentation that the spies could remove from the premises increased reaching a level of hundreds of thousands of documents in a matter of days in the case of Edward Snowden.

5.6.4 Market opportunities

The term, 'market' has been defined as a system that integrates 'the forces of supply and demand for a particular good or service' and that consists of customers, suppliers, and mechanisms for effecting transactions (Imber & Toffler, 2000:342). Related to the subject of this research, the goods are information that the spy provides to the handler and the service is that of espionage. In exchange for these goods and services, the spy receives money and/or some other incentive which may be tangible or intangible (Herbig, 2017:45). In all four cases that have been analysed in this study, market opportunities prevailed which promoted the acts of espionage. In the case of Brian Regan, however, the exchange was never completed only because he was apprehended beforehand.

5.6.4.1 Market opportunities in the Oleg Gordievsky case

By the time Oleg Gordievsky became a spy for MI6, he was a seasoned intelligence officer with 11 years of experience. He continued rising through the system and ultimately achieved the rank of Colonel in the KGB and the role of Resident-designate at the Soviet embassy in London in 1985 shortly before his defection to the West (Andrew, 2009:725-726; MacIntyre, 2018:58). With his rank and assignments came the privilege to access information from the highest levels within his government (MacIntyre, 2018:46). The insights he could offer MI6 with respect to what was being discussed in the Kremlin made Gordievsky an asset of the greatest value (Andrew, 2009:722-723 & 725). Although he was a high-value asset, and undoubtedly aware of this, Gordievsky did not want money or any other tangible benefit in exchange for the information he provided. Gordievsky had an ulterior motive for his actions. He valued freedom, democracy, and justice, and he despised the Soviet system because, in his view, it consistently violated these values (Gordievsky, 2018:11 & 82). His aim, therefore, was to damage the system and contribute to its downfall (Gordievsky, 2018:213). For this, he needed the support of allies. As an ideologically motivated insider spy, the benefit that Gordievsky received in exchange for the information he provided was to see the damage he was able to do to the Soviet system (MacIntyre, 2018:58).

5.6.4.2 Market opportunities in the Aldrich Ames case

When Aldrich Ames offered his services to the KGB, he was, like Oleg Gordievsky, a seasoned intelligence officer with more than 15 years of experience and considerable insights that could be of value to his prospective customers (United States District Court for the Eastern District of Virginia, 1997:4). The fact that Ames could provide his handler vast amounts of documentation made Ames a key supplier for the KGB (Senate Select Committee on Intelligence, 1994:69). The KGB knew that it had leaks in its system. The fact that Ames was able to provide the identities of many of them made Ames an extraordinarily valuable asset. In exchange for the goods and services he provided, the KGB and - after the Cold War - the FSB gave Ames a total of $2.5 million over the nine-year period in which he worked for them (Senate Select Committee on Intelligence, 1994:2).

5.6.4.3 Market opportunities in the Brian Regan case

Through his work as the webmaster of his division at the NRO, Brian Regan had access to tens of thousands of Web pages containing a wide array of secrets that had been gathered by the US intelligence community (Bhattacharjee, 2016:97 & 102). He recognised the market potential that such information would have if he sold it to an enemy state. He identified potential customers for his illicitly gained information, oriented his collection efforts towards these potential customers, and sorted the stolen information into customer-specific containers. To initiate the market transactions, he sent a sample of the stolen material to the Libyan embassy. His plan was to set up transactions with Iran, Iraq, and Sudan as well (Bhattacharjee, 2016:105 & 108-109). He was, however, arrested before he could fully develop his exchange relationships with these countries (Bhattacharjee, 2016:218).

5.6.4.4 Market opportunities in the Edward Snowden case

Edward Snowden wanted to expose the bulk information collection activities of the government to the US public. His work as a computer systems administrator for the NSA gave him access to a vast number of documents that were stored on the servers of the intelligence community. He was able to further broaden his access by getting the logins and passwords from many of his colleagues (Hosenball & Strobel, 2013:n.p.; Snowden, 2019:3). He briefly considered self-publishing but soon decided that this would not achieve the desired outcome (Snowden, 2019:242-246 & 249). To be effective, he needed access to the media platforms that only serious journalists could provide. Realising that journalists compete for ‘scoops’, he would offer a substantial number of documents and ‘provide the technological training and tools to help them do their reporting accurately and safely’ in exchange for their publication of his story (Snowden, 2019:246 & 249). Snowden always insisted that the purpose of his actions was to expose and thereby thwart the activities of the US government. However, whether by design or default, Snowden subsequently became a public speaker, which has brought him honoraria of more than $10,000 per engagement. According to one estimate, he collected more than $200,000 in 2018 alone. In addition, he published his autobiography in 2019, which has been listed as a bestseller (United States District Court for the Eastern District of Virginia, 2019:19-20).

In all four cases, there was a transaction in which the insider spies offered information in exchange for some incentive. In the case of Oleg Gordievsky, it was the alliance with a Western intelligence agency through which he could damage the system he wanted to help bring down. In the cases of Aldrich Ames and Brian Regan, the incentive was money. In Snowden's case, it was, by his own account, the opportunity to expose the actions of the US intelligence community that defined his exchange relationship with the journalists. However, it is noteworthy that he later became active in the speaker's circuit where he received honoraria of more than $10,000 per talk and an estimated $200,000 in 2018 alone. In addition, he published his autobiography in 2019, which has been listed as a bestseller.

Finally, it is interesting to note how developments in the ICT field have impacted the possibilities to establish contact with customers. It took Oleg Gordievsky six years (from 1968 to 1974) to establish contact with MI6. Using the internet, establishing contact only took Edward Snowden a few days.

5.6.5 Disinhibiting factors

Disinhibiting factors reduce or negate an individual's inclination to comply with social norms and these factors include 1) emotional reactions, 2) personality structure, 3) mental disorders, and 4) substance abuse and addictions (American Psychiatric Association, 2013:20; Deckers, 2016:41-47 & 359; Keltner & Shiota, 2003:89). The analysis of the four cases has brought to light that such factors have been present in all four instances.

5.6.5.1 Disinhibiting factors in the Oleg Gordievsky case

Oleg Gordievsky witnessed several events that cumulatively led to a flashpoint. However, it was the Soviet invasion of Czechoslovakia during the Prague Spring that gave him the final push to oppose the Soviet system. He was outraged at what the Soviet state had done and could no longer contain his fury and hatred for the system. Whatever inhibitions he might have previously had to oppose the Soviet state; these were lost with the profound anger that he experienced because of the Soviet invasion of Czechoslovakia. According to his own accounts, it was because of this event that he decided to damage the system through the means he had at his disposal (i.e. espionage) (Gordievsky, 2018:58, 196, 213 & 256-257).

5.6.5.2 Disinhibiting factors in the Aldrich Ames case

Aldrich Ames was driven by the fear of financial ruin and what it would do to his marriage. Ames dismissed legitimate sources of increasing his income from the outset for fear that they would not generate enough money. Consequently, Ames began to consider espionage as the way out of his predicament (Earley, 1997:135). It appears, however, that there was more than just the emotional component that had a disinhibiting effect. There are indications suggesting the presence of an antisocial personality disorder. Ames 1) repeatedly displayed behaviours in which he failed to conform with social and legal norms, 2) was deceitful, 3) repeatedly failed to uphold regular work behaviour or honour financial commitments, and 4) displayed no remorse regarding his deeds (Earley, 1997:37, 130-132 & 145-146; Senate Select Committee on Intelligence, 1994:5, 7-8, 11). In addition to these disinhibiting factors, there is also evidence in Aldrich Ames' personal history that his consummatory behaviour with respect to alcohol affected him and facilitated his recklessness (Earley, 1997:54 & 112-113; Senate Select Committee on Intelligence, 1994:5 & 8).

5.6.5.3 Disinhibiting factors in the Brian Regan case

The case of Brian Regan resembles that of Aldrich Ames in various ways. As in the case of Ames, Brian Regan was driven by the fear of financial ruin and what it would do to his marriage. However, in comparison with Ames, Regan first tried his hand at improving his situation through legal means. He began gambling, trying to peddle his inventions, and investing in the stock market, but these schemes all failed. As his retirement drew closer, he began to panic and consequently considered espionage as the way out of his predicaments (Bhattacharjee, 2016:104-105). As in the case of Ames, it appears there was more than just the emotional component that had a disinhibiting effect. Regan also engaged in behaviours that suggest the presence of an antisocial personality disorder. He 1) repeatedly displayed behaviours in which he failed to conform with social and legal norms, 2) was deceitful, 3) repeatedly failed to sustain consistent work behaviour or honour financial obligations, and 4) displayed a lack of remorse regarding his deeds (Bhattacharjee, 2016:59, 66, 93-94, 96, 102 & 109).

5.6.5.4 Disinhibiting factors in the Edward Snowden case

Edward Snowden was deeply disillusioned by his government and disgusted with the government's actions. He felt that the government had profoundly violated the constitution, which he held dear. Any inhibitions he might have had about breaking the law by disclosing classified information to unauthorised third parties were dispelled by the anger he felt over what in his view was an ongoing injustice (Bamford, 2014:n.p.; Greenwald et al., 2013:n.p.). As in the cases of Aldrich Ames and Brian Regan, there are indications of deceitfulness, recklessness, and lack of remorse in Snowden's history that imply that an antisocial personality disorder may have also been involved and had a disinhibiting effect. There are also indications that a narcissistic personality disorder may have been involved (American Psychiatric Association, 2013:659; Shechter & Lang, 2011:vii).

In all four cases, there were emotional factors that reduced or negated the subjects' inclinations to comply with social norms. Oleg Gordievsky and Edward Snowden were driven by anger. Aldrich Ames and Brian Regan were driven by fear. In addition, the inhibitions of Edward Snowden, Aldrich Ames, and Brian Regan to break the law may also have been compromised by the presence of an antisocial personality disorder. In the case of Aldrich Ames, the adverse effects of excessive alcohol consumption and in the case of Edward Snowden, a narcissistic personality disorder also appear to have played a role.

5.7 VALIDATION OF THE CONCEPTUAL FRAMEWORK

In this chapter, the aim has been to answer the fourth question of this research:

> **Question 4:** How can the interdisciplinary conceptual framework be applied to specific cases of insider espionage to identify the presence of predictors of insider espionage, and thereby validate the conceptual framework?

With the use of the sampling approach outlined in Section 2.3.3, the researcher selected four cases for analysis in an iterative approach consisting of data collection, data analysis, and the write-up of findings (Aurini, Heath & Howells, 2016:19). This process was continued until data saturation was achieved. The earliest of the cases, that of Oleg Gordievsky, dates back to the Cold War in its entirety. The second case, that of Aldrich Ames, began during the Cold War and extended into the post-Cold War period. The cases of Brian Regan and Edward Snowden are both post-Cold War cases. Snowden's case is the most recent and occurred less than a decade ago.

The focus of this chapter was on applying the conceptual framework developed by the researcher to actual cases of insider espionage as a means of validating the conceptual framework itself. Table 5.1 below summarises the variables that have emerged in each of the cases with respect to the five factors (i.e. triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors). This table shows that there was involvement of each of the factors in all four espionage cases and that variables that the researcher associated with each of these factors in Figure 3.3 above were also involved. From the researcher's point of view, this is a promising result because it suggests that the universes of possible variations can, indeed, be captured by the conceptual framework that has been developed by the researcher.

Table 5.1: Summary of variables by case

Case	Triggers	Motives	Situational vulnerabilities	Market opportunities	Disinhibiting factors
Oleg Gordievsky	Predispositions: Values: political, cultural, and spiritual freedom, democracy, and prosperity Triggering Events/Situations: • Treatment of Jews in the Soviet Union under Stalin • Soviet suppression of the Hungarian Uprising • Building of the Berlin Wall • Soviet suppression of the Prague Spring	Emotional reaction: Extreme disgust and anger at the Soviet system Action readiness: Desire to bring the Soviet system down	Information vulnerabilities: High-level access to documents and microfiche films Physical vulnerabilities: Lack of security controls when leaving premises	Supplier: Oleg Gordievsky Customer: MI6 Information: Top-level information regarding the Soviet Union Incentive: Satisfaction of causing damage to the Soviet system	Affect: Extreme disgust and anger at the Soviet system
Aldrich Ames	Predispositions: • Need for affiliation (companionship) • Need for financial security (affluence) Triggering Events/Situations: • Fraying relationship with spouse • Financial strain	Emotional reaction: Fear of separation from his spouse and of financial difficulties Action readiness: To find sources of (illegal) additional income	Personnel vulnerabilities: • Flawed polygraph procedures • Flawed procedures in handling substance abuse Physical vulnerabilities: • Uncontrolled access to offices of colleagues	Supplier: Aldrich Ames Customer: KGB Information: Vast amount of secret information including names of western agents in the Soviet Union	Affect: Extreme fear Mental disorder: Antisocial personality disorder Addiction and substance abuse:

Case	Triggers	Motives	Situational vulnerabilities	Market opportunities	Disinhibiting factors
			• Lack of security controls when leaving premises Information vulnerabilities: Uncontrolled access to copies of documents marked for destruction ICT vulnerabilities: • Uncontrolled access electronic documents • No tracking of document downloads	Incentive: Money	Excessive alcohol consumption, probable alcoholism
Brian Regan	Predispositions: • Need for self esteem • Need for financial security (affluence) Triggering Events/ Situations • Fraying relationship with spouse • Financial strain • Lack of career perspective following retirement	Emotional reaction: Fear of separation from his spouse and of financial difficulties Action readiness: To find sources of additional income	Personnel vulnerabilities: Flawed reinvestigation procedures with respect to personal finances Physical vulnerabilities: Lack of security controls when leaving premises Information vulnerabilities: Uncontrolled access to training video cassettes ICT vulnerabilities:	Supplier: Brian Regan Customer: Intelligence agencies of Iraq, Iran, Libya, and Sudan Information: Vast amounts of information regarding the potential customer nations including satellite reconnaissance imagery	Affect: Extreme fear Mental disorder: Antisocial personality disorder

Case	Triggers	Motives	Situational vulnerabilities	Market opportunities	Disinhibiting factors
			• Uncontrolled access electronic documents on Intelink system • Uncontrolled authorisation to print-out documents from the Intelink system • Unrestricted download of massive amounts of documents onto CD-ROMs	Incentive: Money	
Edward Snowden	Predispositions: • Values: liberty and justice • Value: possibly financially comfortable lifestyle Triggering Events/ Situations: • Bulk data collection on US citizens • False statement by DNI Clapper	Emotional reaction: Intense disillusionment and anger at the US government Action readiness: Desire to expose and thwart the domestic surveillance activities of the government Possibly also to capitalise on his knowledge of governmental secrets	Personnel vulnerabilities: Flawed screening procedures prior to employment Physical vulnerabilities: Lack of security controls when leaving premises ICT vulnerabilities: • Uncontrolled access electronic documents on computer network • Inadequate application of security standards with respect to user account and password information management	Supplier: Edward Snowden Customer: MI6 Information: Vast amounts of information regarding the domestic bulk surveillance program of the US government Incentive: Satisfaction of exposing and thwarting the government activity.	Affect: Intense disillusionment and anger at the US government Mental disorder: Antisocial personality disorder

Case	Triggers	Motives	Situational vulnerabilities	Market opportunities	Disinhibiting factors
			• Unrestricted download of massive amounts of documents onto SD-cards	Possibly also opportunity for personal financial gain	

(Source: Compiled by the researcher)

It is the researcher’s view that the case analyses also demonstrate that the sequence of events as suggested in the conceptual framework occur in the same manner. This means that events or situations that resonate with the predispositions of individuals do create triggers. The triggers then elicit motivation processes which lead to the individual’s action readiness. This, in turn, prompts the individual to actively seek options that are appropriate in the handling of the trigger. The option to commit insider espionage exists if the organisation for which the individual works has vulnerabilities in its security system, and there is a market for the secret information that the individual can illicitly acquire. In finality, however, all these circumstances will only lead to an act of insider espionage if the individual is uninhibited with a view to committing such an act.

CHAPTER 6: FINDINGS, RECOMMENDATIONS AND CONCLUSION

6.1 INTRODUCTION

Insider espionage has destabilised governments, jeopardised national security and infrastructures, diminished the economic strength of nations, and cost lives (Sale, 2003:3-5; Security Service MI5, 2019; Senate Select Committee on Intelligence, 1994:61). Despite the significant damage that insider espionage can cause to a society or organisation, the methods currently used to address this problem are not yet as effective as they should be (Olson, 2019:78). Efforts to combat insider espionage in the governmental and private sectors are aimed fundamentally at deterrence and detection. However, neither of these efforts have produced the desired results. Given the seemingly endless flow of new insider espionage cases that emerge every year, it does not appear that deterrence has been very effective. Similarly, detection has also not produced the desired outcomes because most cases of insider espionage are uncovered through betrayal by some third party, rather than through the application of effective detection techniques (Charney, 2019:37; Prunckun, 2019:25). One of the reasons for the inefficacy of the existing approaches is that they are based on conceptual frameworks that have abundant shortcomings (Charney, 2019:37; Olson, 2019:78).

In this chapter, the researcher essentialises the main findings, recommendations, and conclusion of the study by exclusively focusing on the research questions of this study and their attendant objectives (Yin, 2018:26). In that regard, the researcher reports his findings and articulates the recommendations that he has proposed in tandem with these findings. The researcher further makes suggestions for possible future directions for research relating to insider espionage as a distinct field of study with its conceptual and methodological framework(s), as well as practice-related protocols (Efron & Ravid, 2019:47). The study then concludes in relation to both its main findings and recommendations.

6.2 RESEARCH QUESTIONS

In view of the deficiencies in existing conceptual frameworks of insider espionage, which the researcher has outlined in Subsection 1.3.13 of Chapter 1, the researcher formulated the following four research questions (as articulated in Section 1.5 of Chapter 1):

- **Question 1**: What are the independent variables that are predictors of insider espionage (dependent variable) in the government and private sectors?
- **Question 2**: What are the relationships between the variables of insider espionage in the government and private sectors?
- **Question 3**: How can the variables of insider espionage and the relationships between them be represented in an interdisciplinary conceptual framework that can serve to predict risks of insider espionage?
- **Question 4**: How can this interdisciplinary conceptual framework be applied to specific cases of insider espionage to identify the presence of predictors of insider espionage and thereby validate the conceptual framework?

It is on the basis of these questions that the structure of the research and its direction were developed (Aurini et al., 2016:46). It should also be noted that each of these research questions is closely and sequentially associated with the primary study objectives.

6.3 RESEARCH OBJECTIVES

In tandem with the above-stated research questions, the researcher formulated the four following research objectives that have been addressed during this study:

- To explore the independent variables that are predictors of insider espionage (dependent variable) in the government and private sectors.
- To explore the relationships between the variables of insider espionage in the government and private sectors.
- To construct an interdisciplinary conceptual framework that represents the variables of insider espionage and their relationships, which can serve to predict risks of insider espionage.
- To explore the application of the interdisciplinary conceptual framework to specific cases of insider espionage in order to identify the presence of predictors and thereby validate the conceptual framework.

The research objectives associated with this study have been achieved. The corresponding findings, recommendations, and conclusions are addressed in the following sections.

6.4 FINDINGS

This section is focused on the study's findings, which are reported sequentially in respect of the four research questions as articulated in Section 6.2 above.

6.4.1 Variables that are predictors of insider espionage

The focus of this subsection is on the findings related to the first research question in the study:

> **Question 1**: What are the independent variables that are predictors of insider espionage in the government and private sectors?

The discussion of the findings with respect to this question first addresses those findings that pertain to current approaches to insider espionage, namely: 1) triggers, 2) motives, 3) situational vulnerabilities, 4) market opportunities, and 5) disinhibiting factors.

6.4.1.1 The scope of variables in current approaches to insider espionage

It was found that current approaches to insider espionage discussed in Section 1.3.7. – 1.3.12. offer valuable contributions to our understanding of this phenomenon. However, these approaches were found to be deficient in the following areas: 1) all but one of them capture the full range of factors that lead to insider espionage, 2) within each factor, the constituent elements (variables) are only anecdotally addressed, and 3) the relationship between the factors, which jointly constitute a process leading to insider espionage often remain unclear.

6.4.1.2 Relevance and types of triggers in insider espionage

It was found that nine of the fourteen approaches to insider espionage analysed in this study fail to consider triggers as key factors in the process of becoming an insider spy (see Section 1.3.13.). Consistent with the researcher's conceptual framework, it was also found that:

- Acts of espionage are, in fact, preceded by events or situations that act as triggers. All four cases examined in this study provided evidence to this effect, thus, corroborating this finding;
- The current approaches to insider espionage that do consider triggers, focus on major life events or situations, but do not recognise that events or situations that are more commonplace (e.g. financial strain) can also act as triggers. Consistent with the researcher's conceptual framework, commonplace events or situations can in fact also act as triggers. In two of the four cases analysed in this study, financial strain and fraying marital relations acted as triggers (i.e., the cases of Aldrich Ames and Brian Regan);
- The current approaches to insider espionage that do consider triggers disregard that events or situations at the societal or governmental level can also act as triggers; and
- Societal conditions and governmental policies do, in fact, act as triggers. Evidence of this was provided in two of the four cases analysed in this study (i.e. the cases of Oleg Gordievsky and Edward Snowden).

6.4.1.3 Differences in reactions to events and situations

It was found that those approaches to insider espionage that do consider triggers fail to explain reasons for a given event or situation affecting one individual but not the other. Consistent with the researcher's conceptual framework, it was found in this regard that:

- An individual's reaction to an event or situation depends on the individual's predispositions (i.e., needs, beliefs, values, and ideologies). All cases analysed in this study provided evidence of this.
- Due to their personal histories, the needs of Aldrich Ames and Brian Regan with respect to security (i.e. financial security), affiliation (i.e. marital companionship), and self-esteem (i.e. recognition by peers) were particularly pronounced. Their respective situations jeopardised the fulfilment of these needs and, therefore, acted as triggers.
- Oleg Gordievsky and Edward Snowden held certain values dear (political, cultural, and spiritual freedom, democracy, and prosperity in the case of Gordievsky and

liberty and justice in the case of Snowden). In their assessments, their respective governments were violating these values.

6.4.1.4 Relevance and elements of the motivation process

Consistent with the researcher's conceptual framework, it was found that six of the fourteen existing approaches to insider espionage analysed in this study disregard the role of the motivation process and motives in prompting individual's to become insider spies. It was further found that:

- In all four cases analysed in this study, there had been a motivation process and, therefore a motive, that had led to the acts of espionage;
- None of the current approaches provide and explanation with respect to the motivation process that leads to insider espionage; and
- The motivation process contains an important emotional element that results from the appraisal of the trigger and leads to an individual's action readiness. In all four cases analysed in this study, the individuals concerned had negative appraisals of their respective triggers. These appraisals were followed by strong emotional reactions (fear or anger) and subsequently led to the individuals' action readiness.

6.4.1.5 Relevance and types of situational vulnerabilities

Based on the researcher's conceptual framework, it was found that seven of the fourteen current approaches to insider espionage do not consider situational vulnerabilities as a factor of insider espionage. Additionally, it was also found that:

- Situational vulnerabilities facilitate acts of espionage. All four cases analysed in this study provide evidence of this;
- Of the seven current approaches to insider espionage that consider situational vulnerabilities, none provide a systematic overview of the types of situational vulnerability that can facilitate acts of insider espionage;
- Situational vulnerabilities fall into four categories: personnel vulnerabilities, physical vulnerabilities, information vulnerabilities, and ICT vulnerabilities. Insider espionage can be facilitated by a combination of these vulnerabilities. This was evidenced in all four cases analysed in this study;

- Inadequate personnel security measures (i.e. vetting procedures) prior to, and during employment, played a role in three of the four cases analysed in this study (i.e. Ames, Regan, and Snowden);
- A variety of shortcomings in the physical security set-up enabled the insider spies in all four cases to gain access to information and remove it from their organisational premises;
- Regarding physical security in all four cases analysed in this study, the possibility of being subjected to spot checks by security personnel would have presented the insider spies with the greatest risk of exposure;
- In all four cases analysed in this study, lapses in the procedures of security personnel (i.e. spot checks) enabled the insider spies to remove privileged information from their organisation's premises;
- Vulnerabilities in the information security system (i.e. compartmentalisation, accounting practices, document storage policies, and document and waste disposal policies) enabled the spies in three of the four cases to gain unauthorised access to documents and perform their acts of espionage;
- Regarding developments in the ICT field, it was found that information security system vulnerabilities have profoundly increased the volume of information that could be stolen by insider spies; and
- Deficient (lack of) compartmentalisation of information in the computer systems and the absence of tracking and alert systems when downloading or printing out documents, played a role in three of the four cases of insider espionage (i.e. Ames, Regan, and Snowden).

6.4.1.6 Relevance of market opportunities

Based on the researcher's conceptual framework, it was found that eleven of the fourteen current approaches to insider espionage do not consider market opportunities. In addition, it was also found that:

- Market opportunities play a role in insider espionage. These opportunities require the existence of four variables: 1) a supplier (i.e. insider spy), 2) a customer (i.e. handler), 3) goods and services provided by the supplier (i.e. information) and 4) incentives provided by the customer (tangibles and/or intangibles).
- Evidence of this was found in all four cases analysed in this study.

6.4.1.7 Relevance and types of disinhibiting factors

Similar to the approach applied in the generation of the study's evidence, the researcher's conceptual framework has served as the fundamental framework from which the evidential base of the current study's entire findings. Accordingly, it was found that:

- Eight of the fourteen current approaches to insider espionage do not consider disinhibiting factors as key elements leading to insider espionage;
- There were disinhibiting factors involved in all four cases analysed in this study;
- Of the six current approaches to insider espionage that do consider disinhibiting factors, none offer a complete or systematic overview of the disinhibiting factors that can facilitate insider espionage;
- Disinhibiting factors fall into four categories: 1) emotional response/ affect, 2) personality structure, 3) mental disorder, and 4) addictions and substance abuse;
- Insider espionage is facilitated by reductions of inhibitions. This is evidenced in all four cases.

6.4.2 Relationships between variables that are predictors of insider espionage

The focus of this subsection is on the findings related to the second question of the study:

> **Question 2:** What are the relationships between the variables of insider espionage in the government and private sectors?

6.4.2.1 Relationship between events and situations, and predispositions

It was found that none of the existing approaches to insider espionage address the relationship between events and situations on the one hand and predispositions (needs, beliefs, values and ideologies) on the other. It was found further that:

- Events and situations trigger a response if they resonate with an individual's predispositions.
- The predispositions define the interests of the individual and the events or circumstances that violate (or support) these predispositions, therefore, act as triggers.

- All four cases analysed in this study provided evidence of this.

6.4.2.2 Relationship between triggers and the motivation process

It was found that none of the existing approaches to insider espionage analysed in this study explain how triggers and motivation processes are related. This observation includes the three approaches that consider both variables. In that regard, it was found that:

- Triggers elicit motivation processes that can culminate in the generation of motives.
- All four cases analysed in this study provided evidence of this.

6.4.2.3 Relationship between appraisals, emotional reactions and action readiness

It was found that none of the existing approaches to insider espionage address the variables contained in the motivation process. Furthermore, it was found that:

- The motivation process consists of an appraisal of a trigger, an emotional reaction following the appraisal, and a degree of action readiness that results from the intensity of the emotional reaction.
- In all four cases analysed in this study, the individuals appraised the triggers as being extremely negative. All four subsequently had strong emotional reactions (fear or anger) and were thus willing to engage in some fitness-enhancing, environment-shaping action (i.e. action readiness).

6.4.2.4 Relationship between types of situational vulnerability

It was found that a combination of vulnerabilities relating to personnel, physical layout, information, and/or ICT, rather than a single vulnerability, do enable acts of espionage.

6.4.2.5 Relationship between components of the market exchange

It was found that insider espionage is a market-driven activity which requires the presence of four elements, namely: supplier (insider spy), customer (handler), information (goods and services), and incentives. It is only when all four elements are present that the exchange in an act of espionage can be committed.

6.4.2.6 Relationship between action readiness, situational vulnerabilities, market opportunities, and disinhibiting factors

It was found that the option to engage in acts of espionage exists when: 1) the individual is motivated by a trigger (i.e. reaches a state of action readiness), 2) there are organisational vulnerabilities and market opportunities that can be exploited by the insider spy and 3) the individual is uninhibited with respect to committing acts of espionage. It was further found that these conditions prevailed in all four cases that were analysed in this study.

6.4.3 The interdisciplinary conceptual framework of insider espionage

The focus of this subsection is on the findings pertaining to the third research question of the study, that is:

> **Question 3:** How can the variables of insider espionage and the relationships between them be represented in an interdisciplinary conceptual framework that can serve to predict risks of insider espionage?

Based on the findings outlined in Section 6.4.1 and 6.4.2, Figure 6.1 below depicts the factors, variables, and relationships between the variables as well as the process which leads to insider espionage. This figure lays the foundation for the ensuing discussion on findings related to the third research question.

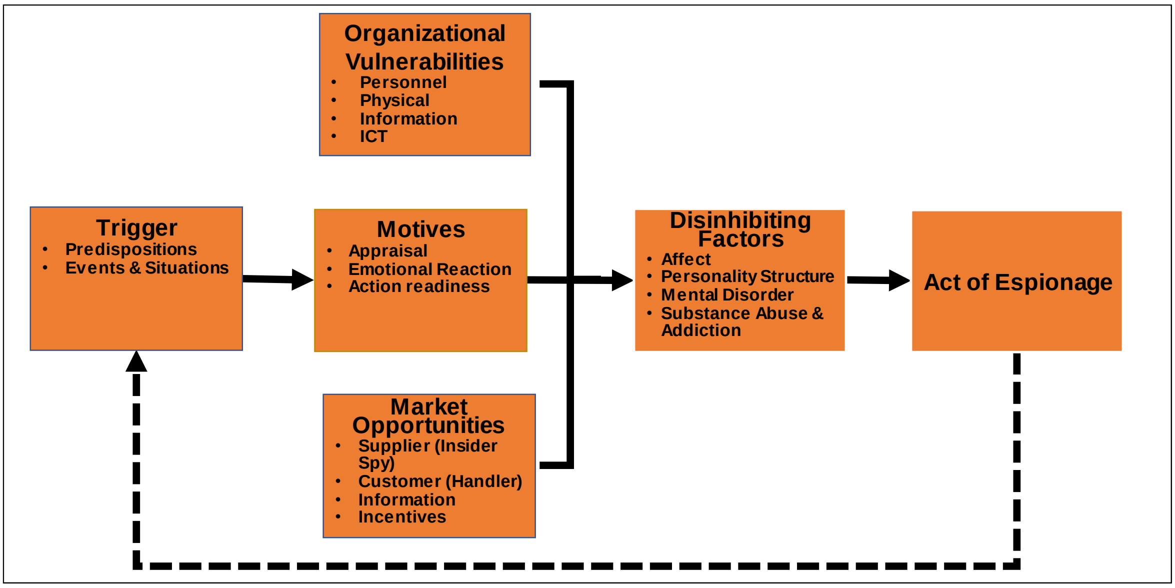


Figure 6.1: Complete conceptual framework of insider espionage

(Source: Developed by the researcher)

It was found that there are five factors that provide an overarching framework to capture the variables of insider espionage. As depicted in Figure 6.1 above, these factors and their interrelated variables are triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors. Based on these, the following findings emerged:

- Triggers are the initial factors at the beginning of the process that ultimately leads to insider espionage;
- The underlying variables associated with triggers are: 1) predispositions (i.e. needs, beliefs, values, and ideologies) and 2) events and situations (stimuli);
- The immediate effect of a trigger is that it initiates a motivation process;
- The underlying variables associated with the motivation process are 1) appraisals, 2) emotional reactions, and 3) action readiness;
- The factor of situational vulnerability is independent of triggers and motives;
- The variables associated with situational vulnerabilities are 1) personnel vulnerabilities; 2) physical vulnerabilities, 3) information vulnerabilities, and 4) ICT vulnerabilities;
- The factor of market opportunity is independent of triggers and motives;
- The variables associated with market opportunities are 1) suppliers (insider spies), 2) customers (handlers), 3) information provided by the insider spy, and 4) incentives provided by the customer (tangibles and/or intangibles);
- Motives, situational vulnerabilities, and market opportunities factor into a decision process, which, if unrestrained by inhibitions, can lead to acts of insider espionage;
- The underlying variables associated with disinhibiting factors are 1) affect, 2) personality structure, 3) mental disorder, and 4) substance abuse and addictions; and
- Acts of espionage can become triggers if the outcomes of the acts are satisfactory, and the potential benefits of committing insider espionage outweigh the potential risks.

6.4.4 Application of the conceptual framework to cases of insider espionage

This section addresses the findings related to the final question of the study:

> **Question 4:** How can this interdisciplinary conceptual framework be applied to specific cases of insider espionage to identify the presence of predictors of insider espionage and thereby validate the conceptual framework?

It was found that the application of the conceptual framework developed by the researcher to specific cases of insider espionage required the review of many more cases than those analysed in this study, because of the varied amount of data that was available with respect to each case. In some instances, available documents related to a case merely consisted of a few brief news reports while in others there was an abundance of material. The researcher found in that regard, that:

- Autobiographies, biographies, and court records, if available, offered a considerable amount of data relevant to the individual cases of insider espionage and to the conceptual framework;
- In-depth analysis of available documents and winnowing were essential processes in answering Question 4 because available texts were so rich with information and only parts of them were useful for the application to the conceptual framework;
- In all four cases, there were triggers at the outset of the process that ultimately led to the individual committing insider espionage;
- In all four cases, there were motivation processes that were marked by negative appraisals and strong negative emotional reactions that culminated in the individual's action readiness;
- In all four cases, the individual's action readiness prompted the individual to consider insider espionage as a response to the trigger;
- In all four cases, there were situational vulnerabilities that facilitated the acts of insider espionage;
- In all four cases, the presence of market opportunities facilitated the acts of espionage;
- In all four cases there were disinhibiting factors that facilitated the acts of espionage; and
- In terms of sequence, it was found that the events in all four cases followed the same pattern in that the process leading to insider espionage was initiated by a trigger which subsequently initiated a motivation process culminating in the individual's action readiness.

Based on all of the afore-mentioned findings in this subsection, it was found that the conceptual framework developed by the researcher has been validated through its application to the four cases.

6.5 RECOMMENDATIONS

The purpose of the present subsection is to provide recommendations in light of the findings that were reported in Section 6.3. Since the study and the reporting of findings were structured in tandem with the four established research questions, the researcher has structured the discussion on recommendations in accordance with the same research questions. Therefore, the recommendations are categorised largely in terms of variables linked to predictors of insider espionage; relationships between variables linked to predictors of insider espionage; the interdisciplinary conceptual framework of insider espionage; application of the conceptual framework to cases of insider espionage; as well as recommendations for future research.

6.5.1 Variables that are predictors of insider espionage

The focus of this subsection is on the recommendations pertaining to the first question of the study, that is:

> **Question 1:** What are the independent variables that are predictors of insider espionage in the government and private sectors?

6.5.1.1 The scope of variables in current approaches to insider espionage

It is recommended that organisations recognise that current counterintelligence programmes rely on existing approaches to insider espionage that are deficient in various ways. Existing approaches typically fail to capture the full range of factors that lead to insider espionage. Moreover, current approaches only anecdotally address the constituent elements (variables) related to the factors rather than to systematically capture the full range of such elements. Finally, existing approaches fail to explain the relationship between the factors, which jointly constitute a process leading to insider espionage. By failing to consider these points, organisations risk being blindsided because their counterintelligence programmes are likely to be based on incomplete conceptual frameworks.

It is then recommended that the organisation's counterintelligence programme should be based on an approach that captures 1) the full range of factors that lead to insider espionage, 2) within each factor, the constituent elements (variables), and 3) the relationships between the factors in order to reduce the likelihood of being caught off-guard by some set of variables that would otherwise enable an individual to engage in insider espionage. Towards this end, it is further recommended that:

- Organisational counterintelligence programmes should be based on a framework that takes five factors into consideration: 1) triggers, 2) motives, 3) situational vulnerabilities, 4) market opportunities, and 5) disinhibiting factors; and
- Organisations should consider the multidisciplinary framework developed by the researcher in this study since it contains a systematic and in-depth analysis of these five factors. The specifics with respect to the application of the five factors in the organisational context will be discussed in the following recommendations.

6.5.1.2 Relevance and types of triggers of insider espionage

It is recommended that organisations should realise that acts of espionage are preceded by events or situations that act as triggers. This is a crucial point because acts of espionage do not occur unless there have been triggers that initiated them. Accordingly, it is recommended that:

- Organisations ought to be aware of the types of events or situations that may act as triggers of insider espionage as well as the individual contingencies that make such an outcome likely;
- Organisations should realise that not only major life events or situations (e.g. divorce, death of a spouse) but also more commonplace events or situations in the personal or organisational setting (e.g. financial strain, fraying marital relations, stagnating career development) as well as societal conditions and governmental policies and actions can act as triggers. By considering such a broad range of events and situations that may have an adverse effect on an individual, organisations are more likely to detect conditions that may prompt an individual to engage in insider espionage;
- Organisation trains its managers to recognise when personal, organisational, societal, or governmental events or situations are having an adverse effect on an

employee and how to handle such circumstances. This is a key consideration for two reasons. First, it is usually the employee's supervisor who knows the employee better than anyone else in the organisation's management structure. This makes the supervisor the person who is best positioned to detect any emerging risks. Second, supervisors cannot be expected to be sufficiently sensitised to recognise possible risks or how to deal with them unless they are adequately trained in this regard; and

- Once trained, supervisors should routinely monitor whether there are any personal, organisational, societal, or governmental events or situations that might have an adverse impact on a co-worker to the point that it could destabilise him or her.

6.5.1.3 Differences in reactions to events and situations

It is recommended that organisations recognise that events and situations affect individuals differently and that the differences in their reactions depend on their predispositions (needs, beliefs, values, and ideologies). For this reason, it is further recommended that:

- Organisations should train their managers to recognise those predispositions among their co-workers that could become relevant in the context of insider espionage.

6.5.1.4 Relevance and elements of the motivation process

It is recommended that organisations realise that insider espionage is preceded by a motivation process. It is through this realisation that organisations improve their ability to recognise when someone is at risk of becoming an insider spy. It is further recommended that:

- Organisations realise that the motivation process culminates in an individual's action readiness which results from the individual's appraisal of a trigger and the individual's subsequent emotional response (anger, fear, sadness, happiness/joy) to the trigger and its appraisal. By raising their awareness in this regard, organisations are more likely to give the emergence of adverse motives on the part of their employees the necessary level of attention;

- The organisation should train its managers to take note and adequately respond when their co-workers are repeatedly and/or continuously expressing negative appraisals of or having strong negative emotional reactions to certain events or situations. This is an important point because it is through the early observation of such indicators that the risk of an individual engaging in some form of counterproductive behaviour may be detected and defused before it becomes a problem;
- The organisation should put the necessary support structures into place to assist managers and personnel with expert advice and counselling in matters that could adversely affect staff and trigger counterproductive work behaviour. Managers and staff should feel safe to reach out to such advisory and counselling services;
- Organisations should put contingency plans in place how to handle employees who have been adversely affected by certain events or situations at the personal, organisational, societal, or governmental level;
- Organisations ought to offer training to employees how best to cope with challenges that can place an undue burden on the individual (e.g. personal financial management, conflict management, stress management). By offering such services, organisations can defuse adverse developments before they escalate and lead to acts of insider espionage; and
- The organisation should put an exit counselling programme into place to ensure that the employee has as positive a transition out of the organisation as possible and is, therefore, not motivated to engage in acts of espionage after leaving the organisation.

6.5.1.5 Relevance and types of situational vulnerabilities

It is recommended that organisations recognise that situational vulnerabilities enable insider spies to commit acts of espionage. In the absence of situational vulnerabilities, espionage would not be possible. It is essential that organisations recognise this because it is only with this realisation that organisations will dedicate the resources necessary to put the measures into place that will counteract the organisation’s vulnerabilities. It is recommended further that:

- Organisations should recognise that situational vulnerabilities fall into four categories: 1) personnel vulnerabilities, 2) physical vulnerabilities, 3) information vulnerabilities, and 4) ICT vulnerabilities. Towards this end, it is also recommended that organisations are aware that the situational vulnerabilities in a specific instance typically involve a combination of these four types of vulnerability. By considering all four categories, organisations can considerably reduce the risk of enabling organisational insiders to become spies. Accordingly, it is recommended further that:

  - Organisations should have the necessary security policies, procedures, and practices in place to ensure a comprehensive security system that includes personnel, physical, informational, and ICT security.

- Organisations should consistently perform rigorous personnel vetting procedures through which they carefully explore all personal vulnerabilities prior to and during employment. Towards this end, it is recommended that organisations perform background checks exploring whether any of the following risks exist prior to employment or have developed since the employee's appointment:
  - Allegiances to unfriendly entities;
  - Foreign influence and preferences;
  - Personal conduct;
  - Financial difficulties;
  - Excessive consumption of alcohol;
  - Drug and substance abuse;
  - Psychological conditions;
  - Criminal behaviour;
  - Inappropriate handling of protected information;
  - Incompatible external activities; and
  - Inappropriate ICT usage.

Where permissible, it is further recommended that:

- Employees handling highly confidential information ought to be subjected to periodic reinvestigations, possibly including full-scope polygraph testing. It is further recommended that questionable or unsatisfactory results should be subject to an in-depth follow-up investigation using a four-eyes principal. These measures are essential because individuals who are at risk of becoming or who have already become insider spies typically display one or more of the listed characteristics. By identifying these characteristics, organisations can put the necessary measures into place to prevent the individual from engaging in espionage (e.g. reassign the individual to less critical tasks until the existing issues are resolved).

- Organisations recognise that lacking physical security measures are frequent contributing factors in facilitating insider espionage. It is, therefore, recommended that organisations have a physical security system in place that has the following features:
  - Secure site design;
  - Protective barriers;
  - Security lighting;
  - Electronic security systems;
  - Access control points;
  - Key control and locking system security; and
  - Security personnel.
- Organisations should particularly focus on reinforcing their controls of staff leaving the premises by security personnel (i.e. spot checks) since lapses in this type of countermeasure are most frequently contributing factors that enable insider espionage. To that effect, security personnel in organisations should regularly perform unannounced and unpredictable spot checks with employees leaving the organization’s premises. Such spot checks are important not only because they are an effective, and often the only method, to discover when someone is attempting to illicitly remove an object from the organisation’s premises, but also because they pose considerable deterrents due to the uncertainties that they create on the part of employees who may be checked.
- Organisations should recognise that information security measures are essential to protect an organisation’s secrets. Therefore, the organisation’s information security system should include the following features:
  - Information classification;
  - Use of code names where appropriate;
  - Compartmentalisation;
  - Accounting practices;
  - Clear desk policies;
  - Document storage policies; and

    - Document and waste disposal policies.

It is only when organisations put these measures into place that they can ensure that privileged information is handled in such a way that it is adequately protected. With respect to ICT security, organisations should recognise the risks that have emerged due to developments in the ICT field. Through these developments, the volume of information that could be stolen by insider spies has profoundly increased. Therefore:

- Organisations ought to recognise that lacking compartmentalisation of information in the computer systems and the absence of a tracking and alert system when downloading or printing out documents is instrumental in insider espionage.
- Organisational ICT security systems should institutionalise policies, procedures, and practices and the most recent technological updates to ensure:
    - **availability** – ensuring that the information resource is available when it is needed, in the right place, and in the prescribed form,
    - **confidentiality** – ensuring that access to the information resource contained in the system can only be accessed by individuals who are authorised to access it,
    - **integrity** – ensuring that the original form or state of the information resource can only be modified by individuals who are authorised to modify it.
- Organisations should develop and implement a control procedure including periodic audits (inspections) to ensure that the implementation of all protective measures with respect to personnel, physical, information, and ICT security are at all times aligned with the existing policies, procedures, and practices. It is only by putting such measures into place that organisations can be sure that the countermeasures against the various situational vulnerabilities have been optimised.

6.5.1.6 Relevance of market opportunities

It is recommended that organisations should recognise that market opportunities are instrumental in facilitating insider espionage. In that regard, it is further recommended that:

- Organisations should recognise that market opportunities require the existence of 1) a supplier (i.e. insider spy), 2) a customer (i.e. handler), 3) goods and services provided by the supplier (i.e. information) and 4) incentives provided by the customer (tangibles and/ or intangibles);
- Organisations should carefully guard their privileged information and perform a risk assessment with respect to the consequences it would have if this information were to fall into the wrong hands;
- Organisations should gather the intelligence necessary to identify competitors (adversaries) who would have an interest to acquire the valuable privileged information of the organisation; and
- Organisations provide staff who are potential targets due to the type of information they handle or contacts they have with training in which they are briefed on the risks and threat vectors.

6.5.1.7 Relevance and types of disinhibiting factors

It is recommended that organisations must realise that disinhibiting factors compromise an individual's self-control and may thus facilitate acts of espionage. It is further recommended that organisations recognise that there are four types of disinhibiting factor: 1) emotional reaction/ affect, 2) personality structure, 3) mental disorder, and 4) addictions and substance abuse. This is an important point because even when supervisors or colleagues notice the presence of such factors in an individual (e.g. uncontrolled anger, asocial behaviour, or frequent excessive drinking), they do not necessarily connect it to the increased risk of espionage. Moreover:

- Supervisors and personnel handling privileged information ought to be trained on how to recognise and handle risk factors among their colleagues including emotional instabilities, stressful work and personal events and situations that may have an adverse effect, as well as indications of strain, emotional or mental disorder, addiction, or substance abuse;
- Organisations, within the boundaries of (labour) legal permissibility, should administer psychological tests to assess individuals with respect to the five dimensions of personality (Openness, Conscientiousness, Extraversion,

‘Agreeableness’, and Neuroticism) to determine whether there are any factors that could render the individual vulnerable to committing insider espionage;

- Organisations should have individuals who are being considered for employment in jobs that involve the handling of highly confidential information, undergo pre-employment psychological assessments to ensure that the individuals are not suffering from any mental disorders that have been associated with insider espionage (i.e. bipolar disorder, antisocial personality disorder, narcissistic personality disorder, borderline personality disorder, psychopathic disorder). In view of the criticality of such a diagnosis, organisations consistently refrain from hiring individuals with such disorders into positions involving the handling of privileged information;
- Organisations should have individuals who handle highly confidential information undergo periodic drug and alcohol tests, preferably unannounced if legally permissible, to assess substance-related risks. It is also recommended that organisations put exploratory measures into place to assess whether employees handling privileged information are affected by an addiction (e.g. gambling) that might compromise their judgement. While the various types of substance abuse and addiction pose a significant risk, they are also treatable; and
- Organisations should have support structures and temporary reassignment protocols in place in the event that an individual does test positively so that he or she has the opportunity to enter a rehabilitation programme and hopefully recover.

6.5.2 Relationships between variables that are predictors of insider espionage

The focus of this subsection is on the recommendations related to the second question of the study, that is:

> **Question 2:** What are the relationships between the variables of insider espionage in the government and private sectors?

6.5.2.1 Relationship between events and situations, and predispositions

It is recommended that organisations realise that events and situations act as triggers when they adversely resonate with an individual’s predispositions. Furthermore:

- Organisations ought to incorporate the considerations related to interrelations between predispositions, events, situations, and potential triggers in their counterintelligence programme. The specifics are outlined in Section 6.4.3. By raising their awareness of the interplay between events and situations on the one hand and the predispositions on the other, organisations will be better prepared to recognise risks when they emerge.
- Prior to a staffing appointment, and periodically during employment, the organisation should explore the features of the position to assess whether it has any aspects that could be in conflict with an incumbent's needs, beliefs, values, or ideologies.
  - whether any need of a candidate or incumbent (e.g. financial security, self-esteem) is jeopardised to the point that this could become a risk for the employing organisation; and
  - whether any of the candidate's or incumbent's beliefs, values, or ideologies are incompatible with any aspect of the foreseen or current position.
- When making policy, strategic, or operational decisions, organisations should consider the effects that these decisions may have on their employees. It is by routinely monitoring these aspects that organisations are likely to detect risks of insider espionage before they actually become a problem.

6.5.2.2 Relationship between triggers and the motivation process

It is recommended that organisations should recognise that triggers elicit motivation processes which may lead to acts of espionage. Therefore, it is recommended that:

- Organisations should recognise that they may unintentionally create triggers and thus elicit motivation processes that could lead to insider espionage.
- While this realisation would not necessarily alter the decision, it may suggest putting additional mitigation measures into place.

6.5.2.3 Relationship between appraisals, emotional reactions, and action readiness

It is recommended that organisations should recognise that the motivation process is a sequence that begins with the appraisal of a trigger which elicits an emotional reaction and culminates in a degree of action readiness. Furthermore:

- Organisations should recognise that the further this motivation sequence unfolds towards the point of action readiness, the greater the risk of an individual engaging in acts of espionage.
- Organisations should recognise the importance of early detection of such a sequence and that they put the appropriate mitigation measures into place. It is, however, also recommended that organisations realise that motives may manifest themselves through any combination of these three interrelated variables (i.e. appraisals, emotional reactions, and action readiness) and that they might not become visible until very late in the sequence. It is, therefore, recommended that espionage risk awareness training programmes of the organisation include the recognition of signals (including weak signals) with respect to all three elements.

6.5.2.4 Relationship between types of situational vulnerability

It is recommended that organisations should recognise that espionage is typically enabled by a combination of situational vulnerabilities. On that basis, it is recommended that organisations should ensure that the necessary security policies, procedures, and practices are in place, and that these measures are integrated into a comprehensive close-meshed security system rather than an assortment of isolated security measures.

6.5.2.5 Relationship between components of the market exchange

In subsection 6.4.2.5, insider espionage was described as a market-driven activity which requires the presence of four elements: supplier (insider spy), customer (handler), information, and incentives and that it is only when all four elements are present that the act of espionage can be committed. This suggests an innumerable assembly of possible threat vectors. In that regard, it is recommended that organisations should identify the most probable threat vectors and formulate threat narratives on this basis. It is further recommended that organisations put comprehensive mitigation measures into place with respect to each of these threat narratives. This approach will enable organisations to stand better chances of disrupting potential market interactions while, at the same time, ensuring the efficiency of the security system.

6.5.2.6 Relationship between action readiness, situational vulnerabilities, market opportunities, and disinhibiting factors

In subsection 6.4.2.6., it was found that the option to engage in acts of espionage exists when 1) the individual is motivated by a trigger (i.e. reaches a state of action readiness), 2) there are organisational vulnerabilities and market opportunities that can be exploited by the insider spy, and 3) the individual is uninhibited with respect to committing acts of espionage. On that basis, it is recommended that the counterintelligence concept of organisations should take all of these considerations into account on the basis of a comprehensive close-meshed conceptual framework. Organisations will then be able to reduce the probability of becoming the targets of insider espionage.

6.5.3 The interdisciplinary conceptual framework of insider espionage

This section is concerned with the recommendations pertaining to the third research question of the study:

> **Question 3:** How can the variables of insider espionage and the relationships between them be represented in an interdisciplinary conceptual framework that can serve to predict risks of insider espionage?

It is recommended that organisations adopt the framework developed in this study by the researcher and adapt it to their specifics thus considering 1) triggers, 2) motives, 3) situational variables, 4) market opportunities, and 5) disinhibiting factors in their counterintelligence concept. By doing so, organisations will be able to design and implement a comprehensive counterintelligence concept that substantially reduces their risk of insider espionage. Furthermore:

- Organisations should engage in an in-depth analysis of each of these factors and relate them to the specifics of their organisation and its employees on the basis of the recommendations outlined in subsections 6.5.1 and 6.5.2.
- In order to optimise the organisation’s counterintelligence concept, the organisation should consider the following with respect to triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors specifically in the context of the organisation.

With respect to triggers, organisations should:

- Consider that triggers result from the interplay between the predispositions (needs, beliefs, values, and ideologies) of employees on the one hand, and events and situations that resonate with these predispositions on the other.
- Consider that triggers initiate motivation processes that may ultimately result in acts of espionage.
- In order to determine whether there is a risk of insider espionage, explore the predispositions of prospective employees prior to their appointment to ascertain whether any of these might be in conflict:
  - the policies, strategies, and operations of the organisation;
  - the tasks they will be expected to perform; and
  - their personal circumstances (e.g. financial difficulties, strained marital relations).
- In order to determine whether there is a risk of insider espionage, in regular intervals explore the predispositions (needs, beliefs, values, and ideologies) of current employees to ascertain whether any of these might conflict with:
  - the policies, strategies, and operations of the organisation;
  - the tasks they are expected to perform; and
  - their personal circumstances (e.g. financial difficulties, strained marital relations).
- Monitor whether new policies, strategies, and/or operations of the organisation may cause an adverse shift with respect to the predispositions of current employees.
- Monitor whether new tasks to be performed by current employees may cause an adverse shift with respect to their predispositions.
- Monitor whether changes in the personal circumstances of current employees may cause an adverse shift with respect to their predispositions.

With respect to motives, it is recommended that organisations should:

- Consider that motives are the result of motivation processes that sequentially consist of appraisals of triggers, emotional reactions to the triggers based on the appraisals, and of action readiness which depends on the intensity of the emotional reaction;

- Put processes into place through which organisations can regularly monitor and assess the motivation processes of their employees;
- Train supervisors, who work most closely with current employees, to recognise if and when the appraisals, emotional reactions, and/or action readiness of an employee with respect to possible triggers may pose a risk of insider espionage; and
- Have examiners (psychologists) who conduct regular periodic assessments of current employees to evaluate the status of their motivation particularly with respect to possible issues in their professional or private lives that could pose a risk of insider espionage.

With respect to situational vulnerabilities, organisations should:

- Consider that situational vulnerabilities enable individuals to commit insider espionage;
- Consider that situational vulnerabilities relate to 1) personnel security, 2) physical security, 3) information security, and 4) ICT security; and
- Scrutinise their security policies, procedures, and processes to identify and mitigate all existing sources of vulnerability based on the considerations outlined in Section 6.5.1.5 above.

With respect to market opportunities, organisations should:

- Consider that insider espionage is a market-driven undertaking that requires four elements: 1) a supplier (insider spy), 2) a customer (handler), 3) information (goods and services), and 4) incentives (tangibles and intangibles);
- Continuously take stock of their privileged information that could be of high value to unauthorised third parties (customers/handlers);
- Assess which third parties would be able and willing to engage in an exchange of information for some kind of incentive; and
- Ascertain whether such incentives might be inducements for employees of the organisation to commit espionage due to their individual situations.

With respect to disinhibiting factors, organisations should:

- Consider that 1) emotional reactions/ affect, 2) personality structure, 3) mental disorder, and 4) addictions and substance abuse can compromise an individual's inhibitions to commit insider espionage; and
- Periodically conduct psychological assessments with respect to these disinhibiting factors to determine whether the individual's inhibitions are in some significant way compromised.

6.5.4 Application of the conceptual framework to cases of insider espionage

This section particularly addresses the recommendations related to the final question of the study, which is:

> **Question 4:** How can this interdisciplinary conceptual framework be applied to specific cases of insider espionage to identify the presence of predictors of insider espionage and thereby validate the conceptual framework?

Recommendations with respect to this question are aimed at two distinct populations: 1) researchers who intend to apply the conceptual framework to the analysis of case histories, and 2) practitioners who intend to apply the framework to specific cases in their organisational context.

With respect to the research community, it is recommended that:

Before embarking on a case analysis based on the conceptual framework provided in this study, researchers should be aware that they will most likely have to review many more cases than they will be able to analyse. This is because the documents that are available with respect to each case are not written with this researcher's conceptual framework in mind. The consequence is that information that is essential for a comprehensive case analysis is often absent. This is particularly true of newspaper articles whose authors frequently only reflect on the motives and other bits of information that might be of interest to the general public. It is, therefore, recommended that researcher's focus their data collection on autobiographies, biographies, and court records since these are the most promising sources of data with respect to all factors contained in the conceptual framework. In this regard, however, it is also recommended that researchers are aware of the necessity to engage in a considerable amount of winnowing because such documents are so rich with information and only parts of them are useful for the application of the conceptual framework.

With respect to the community of practitioners, **it is recommended that**:

They are aware that the application of the conceptual framework developed by the researcher requires the in-depth exploration of the variables in the context of their organisations as well as the systematic consolidation and analysis of data on an individual case basis. This effort, however, becomes much more manageable if the organisational specifics with respect to situational vulnerabilities and market opportunities - which are likely to apply across multiple cases – have already been analysed. On that account, it is recommended that organisations perform the analyses of the situational vulnerabilities and market opportunities early on in the process and to use this as a foundation when embarking on the analysis of individual cases.

6.5.5 Recommendations for future research

It is recommended for researchers to explore the applicability of this conceptual framework with respect to spies who infiltrated an organisation with the intention of committing espionage (as opposed to those considered in this study who decided to become spies after their employment).

It is recommended for researchers to identify suitable psychometric tests that could be used for individual psychological assessments and their utility with respect to the identification of insider espionage risks.

It is recommended for researchers to further explore the needs, beliefs, and values that are most prevalent in motivating individuals to become insider spies.

It is recommended for researchers to explore the impact of interactions with family members and other significant others in an insider spy’s upbringen.

While the case Monica Elfriede Witt was addressed in the present study, it is recommended that researchers further explore whether the conceptual framework advanced in this study helps to explain insider espionage by insiders.

It is recommended for researchers to explore whether the conceptual framework advanced in this study would also have predictive value in cultural and national settings not addressed in this study.

It is recommended that other, independent researchers explore whether they arrive at the same findings outlined in this study.

6.6 CONCLUSION

Espionage is a crime that has destabilised governments, jeopardised national security and infrastructures, diminished the economic strength of a nation, and it has cost lives. In many instances, espionage is perpetrated by individuals who, in the course of their employment, decide to turn against the organisation for which they work by providing unauthorised third parties with their organisation's secret information. These individuals are referred to as insider spies. Governmental and private organisations that are at risk of becoming targets often go to great lengths to deter or detect insider espionage. However, the measures that are put into place often prove to be ineffective. The seemingly endless stream of new cases of insider espionage suggests that deterrence is not working very well. By the same token, most insider spies are unmasked through betrayal and not because the detection methods were effective.

It has been argued that the reason why current deterrence and detection measures are ineffective is because the underlying conceptual frameworks of insider espionage do not adequately explain or predict this phenomenon. The aim of this study has, therefore, been to explore the variables that are predictors of insider espionage. In order to map the range of variables that are addressed in current conceptual frameworks, the researcher conducted a review of pertinent literature in the intelligence field. Through this review, the researcher found that existing approaches to insider espionage can be grouped into five categories: 1) motivational approaches, 2) personality approaches, 3) situational approaches, 4) situation-dispositional approaches, and 5) process approaches.

Through his analysis of the existing approaches, the researcher found that they are all saddled with shortcomings. Firstly, while each approach provides an important contribution to our understanding of the factors that lead to insider espionage, none of them capture the full range of variables. Secondly, the variables considered in many of these approaches are only anecdotally generated rather than the result of a systematic analysis. Thirdly, the relationships between these variables often remain unclear.

Based on his review of existing approaches, the researcher synthesised five concepts (factors) which, in his view, can explain insider espionage. These are: 1) triggers, 2) motives, 3) situational vulnerabilities, 4) market opportunities, and 5) disinhibiting factors. In the researcher's view, these five factors are individually necessary and jointly sufficient to explain insider espionage. The researcher argues, however, that it is only through the consolidation of these factors into a single framework, the systematic grasp of the constituent variables - free of gaps, overlaps and misalignments - and the unambiguous definition and in-depth understanding of the factors and variables, that insider espionage can be understood and acts of insider espionage can be predicted. To arrive at such a framework, the researcher, therefore, set out to answer four pertinent research questions as outlined specifically in Section 1.6 of Chapter 1 and at the beginning of the current chapter.

In order to address the first two questions, the researcher conducted a thorough and systematic analysis of the variables of insider espionage which he structured around the five concepts that he synthesised on the basis of the literature review (i.e. triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors). To perform this analysis, he focussed his attention on relevant literature from the fields of psychology, psychiatry, political science, law, economics, and security studies. It was through this analysis, that the researcher was able to refine the concepts, identify the variables, and develop an understanding of the relationships between the variables. This analysis formed the basis of the theory and ultimately, the conceptual framework that the researcher developed in this study.

The developed conceptual framework itself is his response to the third question. According to the researcher’s conceptual framework, the chain of events that leads to an individual engaging in insider espionage is triggered by an event or situation, which resonates with the individual because of his or her existing predispositions (i.e. needs, beliefs, values, ideologies). This interaction elicits a motivation process in which the individual first appraises the trigger, then has an emotional reaction to it and finally reaches a level of action readiness. At this point, action readiness merely implies that the individual is prepared to respond to the trigger; it does not indicate *how* the individual will respond. Insider espionage becomes viable 1) if there are situational vulnerabilities in the organisation with respect to personnel, physical, information, and ICT security that the insider has identified and can exploit, and 2) if there is a market for the illicitly acquired information that the insider can trade in exchange for money or some other tangible or intangible incentive. However, even if the individual is prepared to respond to the trigger and if insider espionage is viable, it does not necessarily follow that the individual will commit this crime.

Even if the individual has no other option, the individual’s inhibitions to break the law may prevent the act of espionage. Conversely, if the individual’s judgement is disinhibited through intense emotions (affect), personality structure, mental disorder, and/or substance abuse or addiction, the inhibitions of the individual may be compromised thus paving the way to insider espionage.

The fourth question to be answered through this study was based on the application and validation of the researcher’s conceptual framework to specific cases. In the researcher’s view, the case study method was highly suitable for this research because it focusses on the development of an in-depth analysis of events, activities, or processes related to a phenomenon involving several individuals. To select the cases to be analysed, the researcher opted to use theoretical sampling. This sampling approach follows an iterative procedure of data gathering, analysis and further data gathering until the category under investigation reaches the point of ‘saturation’. Theoretical sampling is particularly suitable for exploratory studies when a researcher wishes to study new and largely uncharted areas because it allows for discovery. Most importantly, it allows for researchers to take advantage of fortuitous events – instances in which relations between variables are discovered that may have remained hidden if more conventional methods of sampling had been used.

Based on this sampling approach, the researcher selected four cases: 1) Oleg Gordievsky, 2) Aldrich Ames, 3) Brian Regan, and 4) Edward Snowden. The analysis of these cases revealed that all five factors (i.e. triggers, motives, situational vulnerabilities, market opportunities, and disinhibiting factors) played a role in promoting the subjects' acts of insider espionage. In all four cases, there were events or situations that negatively resonated with the needs or values of the subjects and therefore became triggers that initiated a motivation process. The subjects appraised their respective triggers extremely negatively which brought on a strong emotional reaction (i.e. fear or anger) and thus also a willingness to act (i.e. action readiness). All four subjects actively sought and found situational vulnerabilities in their respective organisations which enabled them to steal and remove secret information from their organisations' premises. They also all were able to identify customers who would be interested in exchanging the illicitly acquired information for an incentive that the insider spy sought. In one of the cases, however, the insider spy (Brian Regan) was apprehended by law officials before he could perform an exchange. Nevertheless, the judgements of all four subjects were affected by certain disinhibiting factors, which, depending on the case, included intense emotions (affect), personality characteristics, likely mental disorders, and alcohol abuse.

During the case analyses, no other variables emerged that appeared to have a bearing on the outcome (i.e. insider espionage). Moreover, reflecting on each of the cases, it appears highly unlikely that insider espionage would have occurred if any of the five factors had been absent. In the researcher's view, this study offers a significant contribution to the body of literature aimed at explaining insider espionage. The study offers a comprehensive framework that takes account of the variables that are individually necessary and jointly sufficient to explain and predict insider espionage. It also provides the necessary insights with respect to the relationships between these variables. By developing this framework, the researcher has provided an important contribution to the body of literature and a foundation for improved deterrence and detection methods.

The present study has shown that even organisations with impermeable counterintelligence systems have been breached because the planning and/or implementation of their security policies, procedures, and practices were flawed. The evidence provided in this study shows that this observation is as relevant to governmental organisations as it is to industry. The reason is that the underlying conceptual frameworks used by organisations to design their counterintelligence systems are incomplete. The researcher asserts that a counterintelligence system can only be effective, and risks of insider espionage can only be predicted, if the counterintelligence system is based on a comprehensive conceptual framework that includes all relevant factors, variables, and processes. The conceptual framework developed by the researcher will help organisations remedy the existing shortcomings. The focus of this study was on governmental intelligence agencies (i.e. KGB, CIA and NRO) and corporations that provide intelligence services to the government (i.e. Dell and Booz Allen Hamilton), which arguably have the most demanding security requirements. Notwithstanding, the conceptual framework, findings, and recommendations, are equally applicable to other governmental and corporate organisations, particularly those handling privileged information. By applying the conceptual framework and implementing the recommendations developed by the researcher, these organisations will finally find themselves substantially less exposed to the risk of insider espionage than they have been in the past.

LIST OF REFERENCES

Adler, E.S. & Clark, R. 2011. *An invitation to social research: How it's done.* 4th edition. Belmont, CA: Wadsworth.

AIVD Algemene Inlichtingen- en Veiligheidsdienst. n.d. *Analysis of vulnerability to espionage*. Available at: https://irp.fas.org/world/netherlands/aivd-vuln.pdf (accessed on: 10 September 2021).

American Psychiatric Association. 2013. *Diagnostic and statistical manual of mental disorders (DSM-5).* 5th edition. Washington, DC: American Psychiatric Association.

American Psychological Association. 2020. *APA dictionary of psychology.* Available at: https://dictionary.apa.org/predictor-variable (accessed on: 03 May 2020).

Andrew, C. 2009. *The defence of the realm.* London: Allen Lane.

Angie, A.D., Connelly, S., Waples, E. & Kligyte, V. 2011. The influence of discrete emotions on judgement and decision-making: A meta-analytic review. *Cognition and Emotion,* 25(8):1393–1422.

Aurini, J.D., Heath, M. & Howells, S. 2016. *The how to of qualitative research.* London: Sage.

Bachner, F. 2018. *Klaus Kuron will mehr.* Available at: https://www.tagesspiegel.de/gesellschaft/die-groesste-spionageaffaere-der-bundesrepublik-die-stasi-konnte-endlich-zuschlagen/22981130-3.html (accessed on: 1 July 2019).

Bamford, J. 2014. *The most wanted man in the world*. Available at: https://www.wired.com/2014/08/edward-snowden/ (accessed on: 27 April 2022).

Barceló, P. 2003. Hannibals Geheimdienst (pp 30-43). In W. Krieger. (Ed.). *Geheimdienste in der Weltgeschichte*. Munich: C.H. Beck.

Barrick, M.R. & Mount, M.K. 1991. The big five personality dimensions and job performance: A meta-analysis. *Personnel Psychology,* 44(1):1-26.

Bayerisches Landesamt für Verfassungsschutz. 2021. *Wirtschaftsspionage.* Available at: https://www.verfassungsschutz.bayern.de/spionageabwehr/wirtschaftsschutz/wirtschaftspionage/index.html (accessed on: 18 September 2021).

BBC, 2021. *Italy Russia arrest: Wife of navy 'spy' reveals dire finances.* Available at: https://www.bbc.com/news/world-europe-56600959 (accessed on: 18 September 2021).

Beck, R.B., Black, L., Naylor, P.C. & Ibo Shabaka, D. 1999. *World history: Patterns of interaction*. Evanston, Ill.: McDougal Littell.

Bennett, R.M. 2003. *Espionage: Spies and secrets.* London: Virgin Books.

Benny, D. 2014. *Industrial espionage.* Boca Raton: CRC Press.

Beynon, J. & Dunkerley, D. 2000. *Globalization: The reader*. New York: Routledge.

Bhattacharjee, Y. 2016. *The Spy who couldn't spell*. New York: New American Library.

Black, C.E. & Helmreich, E.C. 1972. *Twentieth century Europe: A history*. (4th edition). New York: Alfred A. Knopf.

Blinder, A., Turkewitz, J. & Goldman, A. 2019*. Isolated and adrift, an American woman turned toward Iran*. Available at: https://www.nytimes.com/2019/02/16/us/monica-witt-iran.html (accessed on: 11 April 2022).

Borger, J. 2013. *GCHQ and European spy agencies worked together on mass surveillance.* Available at: https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden (accessed on: 27 April 2022).

Bosco, D. 2012. *Espionage in international organizations: Brussels edition.* Available at: https://foreignpolicy.com/2012/09/19/espionage-in-international-organizations-brussels -edition/ (accessed on: 28 December 2019).

Bosshardt, M.J. 2000. Issues in developing a new conceptual framework for the DoD personnel security program. Minneapolis: Personnel Decisions Research Institutes.

Bouchat, C.J. 2007. An introduction to theatre strategy and regional security. Carlisle: US Army War College.

Brandstätter, H. & Opp, K. 2014. Personality traits ('Big Five') and the propensity to political protest: Alternative models. *Political Psychology,* 35(4):515–537.

Branham, L. 2004. 7 Hidden reasons employees leave: How to recognize the subtle signs and act before it's too late. Saranac Lake: AMACOM.

Bromwich, M.R. 1997. *A review of the FBI's performance in uncovering the espionage activities of Aldrich Hazen Ames.* Available at: https://oig.justice.gov/sites/default/files/legacy/special/9704.htm (accessed on: 15 May 2022).

Bundesamt für Verfassungsschutz. 2017. *Economic security: Our topics.* Available at: https://www.verfassungsschutz.de/download/leaflet-2017-02-our-topics.pdf (accessed on: 28 May 2019).

Bundesamt für Verfassungsschutz. 2021. *Begriff und Hintergründe.* https://www.verfassungsschutz.de/DE/themen/spionage-und-proliferationsabwehr/begriff-und-hintergruende/begriff-und-hintergruende_artikel.html#doc679066bodyText1 (accessed on: 18 September 2021).

Bundesministerium des Inneren. 2020. *Abwehr von Spionageaktivitäten in Deutschland.* Available at: https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/spionage/spionage-node.html (accessed on: 17 September 2021).

Bundesregierung, 2018. *Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA).* Available at: http: //www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm (accessed on: 28 September 2021).

Burkett, R. 2013. An alternative framework for agent recruitment: From MICE to RASCLS. *Studies in Intelligence,* March, 57(1):8-17.

Cairncross, A. & Sinclair, P. 1982. *Introduction to economics.* 6th edition. London: Butterworths & Co.

Canadian Security Intelligence Service. 2020. *CSIS public report 2019.* Ottawa: Canadian Security Intelligence Service.

Carlisle, R. 2005. *Encyclopedia of intelligence and counterintelligence*. New York: Taylor & Francis Group.

Center for Development of Security Excellence. 2015. *Introduction to physical security.* Linthicum Heights, MD: Center for Development of Security Excellence.

Central Intelligence Agency. 2020. *The work of a nation.* Available at: https://www.cia.gov/static/c050e9d29b6a04b639f050d6555e35c6/The-Work-of-a-Nation.pdf (accessed on: 16 September 2021).

Charney, D.L. 2014. *NOIR: A white paper.* Lexington: National Office for Intelligence Reconciliation.

Charney, D.L. 2019. Noir white papers: Three-part series of white papers on insider threat, counterintelligence and counterespionage. Lexington: National Office for Intelligence Reconciliation.

Charney, D.L. & Irvin, J.A. 2016. The psychology of espionage. *The Intelligencer: Journal of U.S. Intelligence Studies,* 22(1):71-77.

Cherkashin, V. & Feifer, G. 2005. *Spy handler: Memoir of a KGB officer.* New York: Basic Books.

Cherryholmes, C.H. 1992. Notes on pragmatism and scientific realism. *Educational Researcher,* 21(6):13– 17.

Christensen, C.R., Andrews, K.R. & Bower, J.L. 1978. *Business policy: Text and cases.* Homewood: Richard D. Irwin.

Chu, H. 1996. *Retired engineer gets 2 years in defense espionage case*. Available at: https://articles.latimes.com/1996-04-10/local/me-56800_1_retired-engineer (accessed on: 04 May 2017).

Chuang, S.C. & Hung-Ming, L. 2007. The effect of induced positive and negative emotion and openness-to-feeling in student's consumer decision making. *Journal of Business and Psychology*, (22):65-78.

Cialdini, R. 1984. *Influence: The psychology of persuasion.* New York: William Morrow and Company.

Clark, R.M. 2014. *Intelligence collection.* Los Angeles: Sage.

Collins, J.J. 2005. The Bible after Babel: Historical criticism in a postmodern age. Cambridge: Wm. B. Eerdmans.

Connett, D. 2016. *British American Tobacco accused of corporate espionage in South Africa.* Available at: http://www.independent.co.uk/news/world/africa/british-american-tobacco-accused-of-corporate-espionage-in-south-africa-a6900731 (accessed on: 01 July 2019).

Corbin, J. & Straus, A. 2008. Basics of qualitative research: Techniques and procedures for developing grounded theory. 3rd edition. Thousand Oaks: Sage.

Costa, P.T. & McCrae, R.R. 1985. *The NEO personality inventory.* Odessa: Psychological Assessment Resources.

Cottam, M.L., Dietz-Uhler, B., Mastors, E. & Preston, T. 2010. *Introduction to political psychology.* 2nd edition. New York: Psychology Press.

Craig, J. M. & Piquero, N.L. 2017. Sensational offending: An application of sensation seeking to white-collar and conventional crimes. *Crime and Delinquency,* 63(11):1363–1382.

Creswell, J.W. 2014. *Research design.* 4th edition. Thousand Oaks: Sage.

Creswell, J.W. & Creswell, J.D. 2018. *Research design.* 5th edition. Thousand Oaks, California: Sage Publications.

Creswell, J.W. & Poth, C.N. 2018. *Qualitative inquiry and research design: Choosing among five approaches.* 4th edition. Thousand Oaks, CA: Sage.

Crotty, M. 1998. *The foundations of social research*. London: Sage.

Danesy, F.C. 1994. *Higher education credentials: A guide to educational systems in Europe and North America*. Chichester: John Wiley and Sons.

De Wet, W., Koekemoer, E. & Nel, J.A. 2016. Exploring the impact of information and communication technology on employees' work and personal lives. *SA Journal of Industrial Psychology*, 42(1):1-11.

Deckers, L. 2005. *Motivation: Biological, psychological, and environmental*. 2nd edition. Boston: Pearson.

Deckers, L. 2016. *Motivation: Biological, psychological, and environmental*. 4th edition. Abington: Routledge.

Defense Personnel Security Research Center. 2009. *Espionage and other compromises of national security. Case summaries from 1975 to 2008.* Available at: http://www.dhra.mil/perserec/espionagecases/espionage_cases_august 2009.pdf (accessed on: 16 April 2017).

Denscombe, M. 2019. *Research proposals.* 2nd edition. London: McGraw-Hill Education Ltd.

Department of Defense. 2020. *DoD Information security program: Overview, classification, and declassification.* Available at: https:// .pdf (accessed on: 28 September 2021).

Department of the Army. 2010. *Physical security.* Available at: https://irp.fas.org/doddir/army/attp3-39-32.pdf (accessed on: 26 September 2021).

Der Spiegel. 1988. Guillaume: Wer war der Schurke? *Der Spiegel*, 26 December: 14-21.

Digman, J.M. 1990. Personality structure: Emergence of the five-factor model. *Annual Review of Psychology,* 41(1):417–440.

Director of Central Intelligence. 1990. *Project Slammer interim report.* Available at: https://www.cia.gov/library/readingroom/docs/DOC_0000218679.pdf (accessed on: 16 April 2019).

Director of Central Intelligence. 2003. *Report by the Joint Intelligence Staff: Terminology.* Available at: https://www.cia.gov/library/readingroom/docs/CIA-RDP80R01731R003600070008-2.pdf (accessed on: 12 December 2019).

Director of National Intelligence. 2019. *Economic espionage.* Available at: https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-threat-assessments-mission/ncsc-economic-espionage (accessed on: 28 May 2019).

Dlugos, G. 1981. The relationship between changing value systems, conflicts, and conflict-handling in the enterprise sector. (651-676). In G. Dlugos & K. Weiermair. (Eds). *Management under differing value systems.* Berlin: de Gruyter.

Dorow, W. 1981. Values and conflict behavior: An exploration of conceptual relationships. (Pp. 677-702). In G. Dlugos & K. Weiermair. (Eds). *Management under differing value systems.* BerlIn: Walter de Gruyter.

Dorow, W. 1982. *Unternehmungspolitik.* Stuttgart: Verlag W. Kohlhammer.

Durrheim, P. & Painter, D. 2016. Research design. (Pp. 131-159). In Terre Blanche, M., Durrheim, K. & Painter, D. (Eds.) 2016. *Research in practice: Applied methods for the social sciences.* (2nd edition). Cape Town: Juta.

Earley, P. 1997. Confessions of a spy: The real story of Aldrich Ames. New York: G.P. Putnam's Sons.

Eden, L., 2018. The fourth industrial revolution: Seven lessons from the past. (Pp. 15-34). In R. van Tulder, A. Verbeke & L. Piscitello. (Eds). *International Business in the Information and Digital Age*. Bingley: Emerald Publishing Limited.

Efron, S.E. & Ravid, R. 2019. *Writing literature review. A practical guide.* New York: Guilford Publication.

Eisenhardt, K.M. 1989. Building theories from case study research. *The Academy of Management Review,* October, 14(4):532-550.

Eoyang, C. 1994. Models of espionage. (Pp. 69–91). In T.R. Sarbin, R.M. Carney & C. Eoyang (Eds). *Citizen espionage: Studies in trust and betrayal.* Westport: Praeger.

Eriksen, T.H. 2014. *Globalization: The key concepts*. Oxford: Bloomsbury UK.

ERR News. 2022. *UK daily: Russia increasing spy recruiting efforts in Estonia*. Available at: https://news.err.ee/1608545272/uk-daily-russia-increasing-spy-recruiting-efforts-in-estonia (accessed on: 26 March 2022).

European Space Agency. 2020. *Security regulations.* Available at: https://download.esa.int/docs/LEX-L/Contracts/ESA_REG_004,rev.2_EN.pdf (accessed on: 26 September 2021).

Eysenck, H.J. 1977. *Crime and personality.* London: Routledge.

Eysenck, M.W. & Brysbaert, M. 2018. *Fundamentals of cognition.* 3rd edition. London: Routledge.

Federal Bureau of Investigation. 2019. *Counterintelligence.* Available at: https://www.fbi.gov/investigate/counterintelligence (accessed on: 30 June 2019).

Federal Bureau of Investigation. 2021. *Intellectual property protection.* Available at: https://www.fbi.gov/file-repository/intellectual-property-protection-brochure.pdf/view (accessed on: 17 September 2021).

Federal Bureau of Investigation, n.d. *Counterintelligence.* Available at: https://www.dni.gov/files/NCSC/documents/products/Insider_Threat_Brochure.pdf (accessed on: 15 May 2022).

Ferguson, H. 2004. *Spy handbook.* London: Bloomsbury.

Fischer, B.B. 2000. The vilification and vindication of colonel Kuklinski. *Studies in Intelligence*, 4(3):19-33

Fink, S. 2002. Sticky fingers: Managing the global risk of economic espionage. Chicago: Dearborn Trade.

Fisher, D.C. 2015. *Corporate intelligence.* Memphis: Fisher.

Frazier, E.R., Nakanishi, Y.J. & Lorimer, M.A. 2009. *Security 101: A physical security primer for transportation agencies.* Washington: Transportation Research Board.

Frijda, N.H. 1986. *The emotions.* Cambridge: Press Syndicate of the University of Cambridge.

Frijda, N.H. 2010. Impulsive action and motivation. *Biological Psychology,* 84(3):570-579.

Furgusson, T.G. 1984. *British military intelligence 1870-1914*. Frederick, Md: University Publications Press.

Garofalo, C., Neumann, C. & Velotti, P. 2021. Psychopathy and aggression: The role of emotion dysregulation. *Journal of Interpersonal Violence,* 36(23-24):12640-12664.

Geis, G. 1994. Trade secret theft as an analogue to treason. (Pp. 127-142). In T.R. Sarbin, R.M. Carney & C. Eoyang (Eds.). *Citizen espionage.* Westport, Ct.: Praeger.

Glynn, S. 2017. The hermeneutical human and social sciences. (Pp. 315-339). In B. Babich (Ed.). *Hermeneutic philosophies of social science.* Berlin: De Gruyter.

Glynn, C.J., Herbst, S., O'keefe, G. & Shapiro, R. 1999. *Public opinion.* Boulder: Westview Press.

Gordievsky, O. 2018. *Next stop execution.* London: Lume Books.

Gottfredson, M.G. & Hirschi, T. 1990. *A general theory of crime.* Palo Alto: Stanford University Press.

Gøtzsche-Astrup, O. 2019. Personality moderates the relationship between uncertainty and political violence: Evidence from two large U.S. samples. *Personality and Individual Differences,* 139:102-109.

Government of Canada. 2020. *Espionage and foreign interference.* Available at: https://www.canada.ca/en/security-intelligence-service/corporate/espionage-and-foreign-interference.html (accessed on: 18 September 2021).

Gowan, R. 2018. *Why spies and international organizations are natural allies.* Available at: https://www.worldpoliticsreview.com/articles/24123/why-spies-and-international-organizations-are-natural-allies (accessed on: 28 December 2019).

Greenwald, G. & Gallagher, R. 2014. *New Zealand launched mass surveillance project while publicly denying it.* Available at: https://the intercept.com/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/ (accessed on: 27 April 2022).

Greenwald, G., MacAskill, E. & Poitras, L. 2013. *Edward Snowden: The whistleblower behind the NSA surveillance revelations*. Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistle blower-surveillance (accessed on: 24 April 2022).

Griggs, R.A. & Jackson, S.L. 2020. *Psychology: A concise introduction.* (6th edition). New York: Worth.

Gross, R.D. 2019. *Psychology: The science of mind and behaviour*. London: Hodder Education.

Guba, E.G. 1990. The alternative paradigm dialog (17-30). In E.G. Guba (Ed.). *The paradigm dialog.* Newbury Park, CA: Sage.

Guba, E.G. & Lincoln, Y.S. 1994. Competing paradigms in qualitative research (pp 105- 117). In K. Denzin & Y.S. Lincoln. (Eds). *Handbook of qualitative research.* Thousand Oaks: Sage.

Hage, J. 1972. *Techniques and problems of theory construction in sociology*. New York: John Wiley & Sons.

Haggbloom, S.J., Warnick, R., Warnick, J.E., Vinessa, J.K., Yarbrough, G.L., Russell, T.M., Borecky, C.M., McGahhey, R., Powell, J.L., Beavers, J. & Monte, E. 2002. The 100 most eminent psychologists of the 20th century. *Review of General Psychology,* 6(2):139-152.

Harding, L. 2018. *How Russian spies bungled cyber-attack on weapons watchdog.* Available at: https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog (accessed on: 05 December 2018).

Hare, R.D., Neumann, C.S. & Mokros, A. 2018. The PCL-R assessment of psychopathy: Development, properties, debates, and new directions (Pp. 39–79). In C.J. Patrick, (Ed.). *Handbook of Psychopathy*. New York: The Guilford Press.

Harvard Law School. 2019. *International Organizations (IGOs).* Available at: https://hls.harvard.edu/dept/opia/what-is-public-interest-law/public-service-practice-settings/public-international-law/intergovernmental-organizations-igos/ (accessed on: 28 December 2019).

Hayes, N. 1994. *Foundations of psychology.* Walton-on-Thames: Thomas Nelson & Sons.

Heinrich-Böll-Stiftung & Schönenberg, R. 2013. *Transnational organized crime: Analyses of a global challenge to democracy*. Bielefeld: Transcript Verlag.

Heneman, H.G., Judge, T.A. & Kammeyer-Mueller, J.D. 2019. *Staffing organizations.* 7th edition. Middleton, WI: McGraw-Hill.

Herbig, K.L. 2008. *Changes in espionage by Americans:1947-2007.* Monterey: Department of Defense.

Herbig, K.L. 2017. *The Expanding spectrum of espionage by Americans, 1947–2015,* Seaside, California: Defense Personnel and Security Research Center.

Hesse-Biber, S.N. & Leavy, P. 2011. *Practice of qualitative research.* 2nd edition. Los Angeles: Sage.

Heuer, R.J. 1994. *Drug use and abuse: Background information for security personnel,* Monterey: Defense Personnel Security Research Center.

Heuer, R.J. 2001. *The insider espionage threat.* Available at: https://www.wrc.noaa.gov/wrso/security_guide/insider.htm (accessed on: 8 April 2017).

Hewstone, M., Finchham, F.D. & Foster, J. 2005. *Psychology*. Malden: BPS Blackwell.

Heywood, A. 2017. *Political ideologies: An introduction.* 6th edition. London: Pelgrave.

Hicks, B.M. & Drislane, L.E. 2018. Variants ('subtypes') of psychopathy. (Pp. 299-332). In C.J. Patrick. (Ed.). *Handbook of Psychopathy.* (2nd edition). New York: The Guilford Press.

Hillier, B. 1968. Pottery and porcelain 1700-1914. England, Europe and North America. London: Weidenfeld & Nicolson.

Hollander, E.P. 1967. *Principles and methods of social psychology.* Oxford: Oxford University Press.

Hollin, C. 1992. *Criminal behaviour: A psychological approach to explanation and prevention*. Hove: Psychological Press.

Hosenball, M. 2013. *NSA contractor hired Snowden despite concerns about resume discrepancies*. Available at: https://www.reuters.com/article/us-usa-security-snowden-idUSBRE95K01J20130621 (accessed on: 26 April 2022).

Hosenball, M. & Strobel, W. 2013. *Snowden persuaded other NSA workers to give up passwords - sources*. Available at: https://www.reuters.com/article/net-us-usa-security-snowden/exclusive-snowden-persuaded-other-nsa-workers-to-give- up-passwords-sources-idUSBRE9A703020131108 (accessed on 27 April 2022).

Houben, M. 2003. Agentinnen aus Liebe – psychologische Betrachtung der Romeomethode (Pp. 247-294). In S.M. Litzcke. (Ed.). *Nachrichtendienstpsychologie 1: Schriftenreihe des Fachbereichs Öffentliche Sicherheit.* Brühl: Fachhochschule des Bundes für öffentliche Verwaltung Fachbereich Öffentliche Sicherheit.

Howell, K.E. 2013. *An Introduction to the philosophy of methodology*. Los Angeles: Sage.

IBM. 2022. *Chronological history of IBM.* Available at: https://www.ibm.com/ibm/history/history/history_intro.html (accessed on: 18 March 2022).

Imber, J. & Toffler, B.A. 2000. *Dictionary of marketing terms.* 3rd edition. Hauppauge: Barron's.

International Chamber of Commerce - Austria, 2021. *Wirtschaftsspionage.* Available at: https://www.icc-austria.org/en/Service/Prevention-of-commercial-crime/Wettbewerbsspionage.htm (accessed on: 18 September 2021).

Israel, R.C. 2012. *What does it mean to be a global citizen?* Available at: https://www.kosmosjournal.org/article/what-does-it-mean-to-be-a-global-citizen/ (accessed on: 13 March 2022).

Izard, C.E. 1993. Four systems for emotion activation: Cognitive and noncognitive processes. *Psychological Review,* 100:68-90.

Jaccard, J. & Jacoby, J. 2010. *Theory construction and model-building skills.* New York: Guilford Press.

Johnson, L.K. 2010. The Oxford Handbook of national security intelligence. New York: Oxford University Press.

Johnson, L.K. 2014. The Evolution of intelligence studies. (Pp. 3-22). In R. Dover, M.S. Goodman & C. Hillebrand. (Eds). *Routledge companion to intelligence studies.* London: Routledge.

Johnson, W.R. 2009. *Thwarting enemies at home and abroad.* Washington, D.C.: G Press Georgetown University.

Kaya, A. 2021. Islamist and nativist reactionary radicalisation in Europe. *Politics and Governance,* 9(3):204-214.

Keck, Z. 2014. Edward Snowden vs New Zealand. Available at: https://thediplomat.com/2014/09/edward-snowden-vs-new-zealand/ (accessed on: 27 April 2022).

Keltner, D. & Shiota, M.N. 2003. New displays and new emotions: A Commentary on Rozin and Cohen. *Emotion,* 3(1):86–91.

Kent, S. 1966. *Strategic intelligence for American world policy.* Princeton: Princeton University Press.

Khrushchev, N. 1971. *Khrushchev remembers.* London: André Deutsch Limited.

Killam, L.A. 2013. *Research terminology simplified: Paradigms, axiology, ontology, epistemology, and methodology*. Sudbury, Ontario: Author.

Kleiner, F.S. 2016. *Gardner's art through the ages.* (15th edition). Boston: Cengage.

Kluckhohn, C. 1951. Values and value-orientations in the theory of action: An exploration in definition and classification. (Pp. 388-433). In T. Parsons & E. Shils. (Eds). *Toward a General Theory of Action.* Cambridge: Harvard University Press.

Koot, M.R. 2022. *Dutch intelligence service warns public about online recruitment by foreign spies.* Available at: https://intelnews.org/2022/02/15/01-3152/ (accessed on: 28 March 2022).

Leavy, P. 2017. *Research design.* New York: Guilford Publications.

Lerner, J.S. & Keltner, D. 2001. Fear, anger, and risk. *Journal of Personality and Social Psychology,* 8(1):146–159.

Leslie, T. & Corcoran, M. 2013. *Australia's involvement with the NSA, the US spy agency at heart of global scandal*. Available at: https://www.abc. net.au/news/ 2013-11-08/australian-nsa-involvement-explained/5079786?nw=0&r=Map (accessed on: 27 April 2022).

Levchenko, S. 1988. *On the wrong side: My life in the KGB.* New York: Pergamon.

Lincoln, Y.S. & Guba, E.G. 1985. *Naturalistic inquiry.* Newbury Park: Sage.

Lincoln, Y.S. & Guba, E.G. 2013. *The constructivist credo.* New York: Routledge.

Lipson, L. 1977. *The great issues of politics.* 5th edition. Englewood Cliffs: Prentice-Hall.

Lucas, E. 2018. *Spycraft rebooted: How technology is changing espionage*. Kindle ed. Seattle: Amazon Publishing.

Maass, P. 2013. *How Laura Poitra helped Snowden spill his secrets.* Available at: https://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html (accessed on: 25 April 2022).

MacIntyre, B. 2018. *The spy and the traitor.* Milton Keynes: Penguin Books.

Marsh, A.A. 2013. What can we learn about emotion by studying psychopathy? *Frontiers in Human Neuroscience,* 7:1-13.

Maryland State Archives, 2022. Two acts of toleration: 1649 and 1826. Available at: https://msa.maryland.gov/msa/speccol/sc2200/sc2221/000025/html/intro.html (accessed on: 25 April 2022).

Maslow, A.H. 1970 (1987). *Motivation and personality.* Uttar Pradesh: Pearson.

MaxQDA, 2019. *MaxQDA Training.* Available at: https://www.maxqda.com/training (accessed on: 30 October 2019).

May, E. R., 1995. Studying and teaching Intelligence. *Studies in Intelligence*, 36:1-5.

McClelland, D. 1987. *Human motivation.* Cambridge: Cambridge University Press.

Mehan, J.E. 2016. *Insider threat.* Cambridgeshire: IT Governance.

Milne, S. & MacAskill, E. 2015. *Africa is new 'El Dorado of espionage', leaked intelligence files reveal.* Available at: https://www.theguardian.com/world/2015/feb/24/africa-el-dorado-espionage- leaked-intelligence-files (accessed on: 15 May 2022).

Moore, A., Savinda, J., Monaco, E., Moyes, J., Rousseau, D., Perl, S., Cowley, J., Collins, M., Cassidy, T., VanHoudnos, N., Buttles-Valdez, P., Bauer, D. & Parshall, A. 2016. *The critical role of positive incentives for reducing insider threats.* Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=484917 (accessed on: 05 June 2021).

Müllner, J. & Filatotchev, I. 2018. The changing face of international business in the information age. (Pp. 91–121). In R. van Tulder, A. Verbeke & L. Piscitello. (Eds). *International business in the information and digital age.* Bingley: Emerald Publishing Limited.

Nasheri, H. 2005. *Economic espionage and industrial spying.* Cambridge: Cambridge University Press.

National Archives. 2021. *§ 121.1 The United States Munitions List.* Available at: https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121/subject-group-ECFR6cf5c989d9a8d36/section-121.1 (accessed on: 18 September 2021).

National Cybersecurity and Communications Integration Center. 2014. *Combating the insider threat.* Available at: https://us-cert.cisa.gov/sites/default/files/publications/Combating%20the%20Insider%20 Threat.pdf (accessed on: 22 September 2021).

National Institute of Standards and Technology. 2021. *Vulnerability.* Available at: https://csrc.nist.gov/glossary/term/countermeasures (accessed on: 22 September 2021).

Navarrete, I.M. & Buchan, R. 2019. Out of the legal wilderness: Peacetime espionage, international law and the existence of customary exceptions. *Cornell International Law Journal*, 51(4):897-953.

New International Version. *Holy Bible*, 2011. London: Hodder & Stoughton.

Newell, B.R., Lagnado, D.A. & Shanks, D.R. 2015. *Straight choices: The psychology of decision making.* East Sussex: Psychology Press.

NFP. 2022. *Poland expels 45 Russian spies pretending to be diplomats and arrests espionage suspect.* Available at: https://notesfrompoland.com/2022/03/23/poland-expels-45-russian-spies-pretending-to-be-diplomats-and-arrests-espionage-suspect (accessed on: 26 March 2022).

Nicholls, D., Mikhailova, A. & Luhn, A. 2018. *Russian spies in new humiliation as hundreds of GRU agents' names found online.* Available at: https://www.telegraph.co.uk/news/2018/10/05/putins-spies-new-humiliation-sloppy- procedures-allow-305-gru/ (accessed on: 05 October 2018).

Nolen-Hoeksema, S., Frederiksen, B.L., Loftus, G.R. & Lutz, C. 2014. *Atkinson & Hilgard's introduction to psychology.* (16th edition)*.* Andover: Cengage Learning.

Olson, J.M. 2019. *To catch a spy: The art of counterintelligence.* Washington, D.C.: Georgetown University Press.

Omand, D. 2014. The cycle of intelligence. (Pp. 59-70). In R. Dover, M.S. Goodman & C. Hillebrand. (Eds). *Routledge companion to intelligence studies.* Oxfordshire: Routledge.

Ortony, A. & Turner, T.J. 1990. What’s basic about basic emotions? *Psychological Review,* 93(3):315-331.

Osnos, P. 1982. *Passed Soviets secrets.* Available at: https://www.washingtonpost.com/archive/politics/1982/11/11/passed-soviets-secrets/3e2e1a3f-dd5b-42d4-b8c3-0c4d5eedf0ca/?utm_term=.490a1a22f9f2 (accessed on: 30 June 2019).

Parliament of Australia. 2018. *National security legislation amendment (Espionage and Foreign Interference) Act 2018.* Available at: https://www.legislation.gov.au/Details/C2018A00067/Controls/ (accessed on: 14 December 2019).

Parliament UK. 1981. *Mr. Leo Long.* Available at: https://api.parliament.uk/historic-hansard/written-answers/1981/nov/09/mr-leo-long-1 (accessed on: 14 December 2021).

Pfeiffer, J. 1997. *New directions for organization theory: Problems and prospects*. Oxford: Oxford University Press.

Pincher, C. 1987. *Traitors: The anatomy of treason.* New York: St. Martin's Press.

Prados, J. 2014. *The John Walker spy ring and the U.S. Navy’s biggest betrayal.* Available at: https://news.usni.org/2014/09/02/john-walker-spy-ring-u-s-navys-biggest-betrayal (accessed on: 19 May 2019).

Prunckun, H. 2012. *Counterintelligence: Theory and practice.* Lanham, Md.: Rowman & Littlefield.

Prunckun, H. 2019. *Counterintelligence theory and practice.* London: The Rowman & Littlefield Publishing Group.

Putwain, D. & Sammons, A. 2003. *Psychology and crime.* East Sussex: Routledge.

Reilly, W. & Joyal, P. 1993. Project Slammer: A critical look at the Director of Central Intelligence Directive No. 1/14 criteria, Washington: Director of Central Intelligence.

Reinisch, A. 2009. *Convention of privileges and immunities.* Available at: https://legal.un.org/avl/pdf/ha/cpiun-cpisa/cpiun-cpisa_e.pdf (accessed on: 28 December 2019).

Resnik, D.B. 2015. *What is ethics in research & why is it important?* Available at: https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm (accessed on: 1 October 2019).

Rettman, A. 2019. *Belgian spy scandal puts EU and NATO at risk.* Available at: https://euobserver.com/foreign/144178 (accessed on: 28 December 2019).

Richelson, J.T. 1988. *Foreign intelligence organizations*. Cambridge. Balligner Publishing Company.

Richelson, J.T. 1995. A century of spies: Intelligence in the twentieth century. Oxford: Oxford University Press.

Richelson, J.T. 2016. *The US intelligence community*. Boulder: Worldview Press.

Robertson, R. 1992. *Globalization: Social theory and global culture*. London: Sage.

Rokeach, M. 1968. *Beliefs, attitudes, and values.* San Francisco: Jossey-Bass.

Rokeach, M. 1973. *The nature of human values.* New York: The Free Press.

Rokeach, M. 1979. From individual to institutional values: With special reference to the values of science. (Pp. 47-70). In M. Rokeach. (Ed.). *Understanding human values: Individual and societal.* New York: The Free Press.

Roseman, I.J. & Smith, C.A. 2001. Appraisal theory: Overview, assumptions, varieties, and controversies. (Pp. 3-19). In K.R. Scherer, A. Schorr, & T. Johnstone. (Eds). *Appraisal processes in emotion: Theory, methods, research.* Oxford: Oxford University Press.

Rosenberg, S. 2019. *Putin: Russia foiled work of almost 600 spies.* Available at: https://www.bbc.com/news/world-europe-47467823 (accessed on: 2019 November 2019).

Ross, C.E. & Mirowsky, J. 1979. A comparison of life-event-weighting schemes: Change, undesirability, and effect-proportional indices. *Journal of Health and Social Behavior,* 20(2):166-177.

Rowell, A. & Aviram, A. (2021). *British American Tobacco in South Africa: Any Means Necessary.* Available at: https://bat-uncovered.exposetobacco.org/wp-content/uploads/2021/09/BAT-in-South-Africa.pdf (accessed on: 30 January 2021).

Royal Canadian Mounted Police. 2018. *Strategic priorities.* Available at: http://www.rcmp-grc.gc.ca/prior/index-eng.htm (accessed on: 30 June 2019).

Sale, R. 2003. *Traitors.* New York: Berkley Publishing Group.

Scally, D. 2008. *'Catastrophic' situation after Estonian unmasked as spy.* Available at: https://www.irishtimes.com/news/catastrophic-situation-after-estonian-unmasked-as-spy-1.912030 (accessed on: 28 December 2019).

Schaeffer, R.K. 1997. *Understanding globalization*. Lanham: Rowman & Littlefield.

Schindler, J.R. 2016. *NATO's big new Russian spy scandal.* Available at: https://observer.com/2016/05/natos-big-new-russian-spy-scandal/ (accessed on: 28 December 2019).

Schmid, F. & Ulrich, A. 2010. *New documents reveal truth on NATO's 'Most damaging' spy.* Available at: https://www.spiegel.de/international/europe/betrayer-and-betrayed-new-documents-reveal-truth-on-nato-s-most-damaging-spy-a-693315.html (accessed on: 28 May 2019).

Schopenhauer, A. 1841 *Essay on the freedom of the will.* (Kindle edition published in 2005). Mineola: Dover Publications.

Schreier, M. 2012. *Qualitative content analysis in Practice*. London: Sage.

Schriber, R.A., Chung, J.M., Sorensen, K.S. & Robins, R.W. 2017. Dispositional contempt: A first look at the contemptuous person. *Journal of Personality and Social Psychology,* 113(2):280.

Schug, R.A. & Fradella, H.F. 2015. *Mental illness and crime.* Los Angeles: Sage.

Secretary of the Air Force, 2019. *Information protection.* Available at: https://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1401/afi16-1401.pdf (accessed on: 28 September 2021).

Secretary of the Air Force, 2020. *Operations security (OPSEC).* Available at: https://static.e-publishing.af.mil/production/1/af_a3/publication/afi10-701/afi10-701.pdf (accessed on: 20 August 2021).

Security Service MI5. 2019. *Espionage.* Available at: https://www.mi5.gov.uk/espionage (accessed on: 30 June 2019).

Security Service MI5, 2021. *Introduction to targets of espionage.* Available at: https://mi5.gov.uk/targets-of-espionage (accessed on: 17 September 2021).

Senate Select Committee on Intelligence. 1994. *An assessment of the Aldrich H. Ames espionage case and its implications for U.S. Intelligence.* Available at: https://fas.org/irp/congress/1994_rpt/ssci_ames.htm (accessed on: 24 April 2017).

Shannon, E. 2001. *Death of the perfect spy.* Available at: http://content.time.com/time/magazine/article/0,9171,164863,00.html (accessed on: 28 May 2019).

Shechter, O.G. & Lang, E.L. 2011. *Identifying personality disorders that are security risks: Field test results.* Monterey: Defense Personnel Security Research Center.

Sheldon, R.M. 1989. *Spying in Mesopotamia. Studies in intelligence.* 33 (Spring, 1989):7-12.

Shiraz, Z. 2017. Globalisation and intelligence. (Pp. 265-280). In R. Dover, H. Dylan & M. Goodman. (Eds). *The Palgrave handbook of security, risk, and intelligence*. London: Palgrave Macmillan.

Shoemaker, P.J., Tankard, J.W. & Lasorsa, D.L. 2003. *How to build social science theories*. Thousand Oaks: Sage.

Siegel, L. J., 2017. *Criminology - The Core.* 6th ed. Boston: Cengage Learning.

Simon, H. 1972. Theories of bounded rationality. (Pp. 161-176). In C.B. McGuire & R. Radner. (Eds). *Decision and organization*. Amsterdam: North-Holland Publishing Company.

Slife, B.D. & Williams, R.N. 1995. *What's behind the research? Discovering hidden assumptions in the behavioral sciences*. Thousand Oaks, CA: Sage.

Smith, C.A. & Ellsworth, P.C. 1985. Patterns of cognitive appraisal in emotion. *Journal of Personality and Social Psychology,* 48:813-838.

Smith, M. 2017. *The anatomy of a traitor: The history of espionage and betrayal*. London: Quarto.

Smith, W.T. 2003. *Encyclopedia of the central intelligence agency*. New York: Facts on File.

Sneiderman, P., Slater, E. & Glionna, J.M. 1995. *Ex-aerospace worker indicted in spy case.* Available at: https://articles.latimes.com/1995-05-26/local/me (accessed on: 04 May 2017).

Snowden, E. 2019. *Permanent record.* London: MacMillan.

Snyckers, T. 2021. *BAT's UK headquarters oversaw and financed a South African spy ring*. Available at: https://www.occrp.org/en/investigations/bats-uk-headquarters-oversaw-and-financed-a-south-african-spy-ring (accessed on: 30 January 2023).

Sontheimer, M. 2014. *Wie auf einer Insel.* Available at: https://www.spiegel.de/spiegel/print/d-128101521.html (accessed on: 28 December 2019).

Staatliche Porzellan-Manufaktur Meissen. 2021. *Erfindung des ersten europaeischen Prozellans.* Available at: https://www.meissen.com/de/geschichte (accessed on: 21 February 2021).

Sternberg, R.J. & Sternberg, K. 2017. *Cognitive psychology.* 7th edition. Boston: Cengage Learning.

Strauss, A. & Corbin, J. 1998. *Basics of qualitative research.* 2nd edition. Thousand Oaks, Ca: Sage.

Sulick, M.J. 2013. *American spies.* Washington, D.C.: Georgetown University Press.

Taylor, S.A. 2007. Definitions and theories of counterintelligence. (1-13). In L.K. Johnson. (Ed.). *Strategic intelligence - volume 4: Counterintelligence and counterterrorism.* Newport, CT: Praeger Security International.

Thompson, W.R. 2008. Measuring long-term processes of political globalization. (58-86). In G. Modelski, T. Devezas & W.R. Thompson. (Eds). *Globalization as evolutionary process: Modeling global change*. London: Routledge.

Thornton, M. 1984. *FBI agent charged in espionage.* Available at: https://www.washingtonpost.com/archive/politics/1984/10/04/fbi-agent-charged-in-espionage/2621bd62-08dd-42e5-8b18-6f5bc48a1991/?utm_term=.ed 2aa5e2a1fb (accessed on: 08 May 2017).

Tiedens, L.Z. & Linton, S. 2001. Judgment under emotional certainty and uncertainty: The effects of specific emotions on information processing. *Journal of Personality and Social Psychology,* 81(6):973-988.

Trahair, R.C. 2004. *Encyclopedia of cold war espionage, spies, and secret operations*. Westport, CT: Greenwood Press.

Tsolkas, A. & Wimmer, F. 2013. *Wirtschaftsspionage und intelligence gathering.* Wiesbaden: Springer Verlag.

U.K. Parliament. 2021. *Oleg Gordievsky - volume 570: Debated on Thursday 7 March 1996.* Available at: https://hansard.parliament.uk/Lords/1996-03-07/debates/0d375936-832d-4ecd-80df-8f7819c8b99e/OlegGordievsky (accessed on: 31 October 2021).

United States Congress. 1996. *Economic Espionage Act 1996.* Available at: https://www.govinfo.gov/content/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf (accessed on: 2018 October 2018).

United States District Court for the District of Columbia. 2018. *Indictment – Monica Elfriede Witt.* Available at: https://games-cdn.washingtonpost.com/notes/prod/default/documents/ada2937c-ef1d-4ac8-b91e-1c7a80b86ce6/note/0bdf5c72-b61e-4ebc-8ae7-bf05e0cfe8da.pdf (accessed on: 23 May 2020).

United States District Court for the Eastern District of Virginia. 1997. United States of America v. Aldrich Hazen Ames and Maria Del Rosario Casas Ames: Affidavit in support of criminal complaint, arrest warrants and search warrants. Available at: https://cryptome.org/jya/ames.htm (accessed on: 19 October 2021).

United States District Court for the Eastern District of Virginia. 2001a. *Indictment – Brian Patrick Regan.* Available at: https://irp.fas.org/ops/ci/regan_complaint.html (accessed on: 21 April 2022).

United States District Court for the Eastern District of Virginia. 2001b. *United States of America v. Brian Patrick Regan.* Available at: https://irp.fas.org/ops/ci/regan_indict.html (accessed on: 21 April 2022).

United States District Court for the Eastern District of Virginia. 2013. *United States of America v. Edward J. Snowden.* Available at: https://sgp.fas.org/jud/snowden/complaint.pdf (accessed on: 24 April 2022).

United States District Court for the Eastern District of Virginia. 2019. *United States of America v. Edward Snowden.* Available at: https://justice.gov/usao-edva/press-release/file/1203231/download (accessed on: 24 April 2022).

United States Government. 2017. National security adjudicative guidelines. Available at: https://SEAD-4-Adjudicative-Guidelines-forSecurityClearances.pdf (accessed on: 03 October 2021).

University of Liverpool. 2022. *Cyber security MSc – Online course*. Available at: https://online.liverpool.ac.uk/programmes/msc-cyber-security/ (accessed on: 26 April 2022).

University of South Africa. 2016. *Policy on research ethics.* Available at: https://www.unisa.ac.za/static/corporate_web/Content/Library/Library%20services/ (accessed on: 28 June 2019).

United Nations Convention against Transnational Organized Crime. 2010. *List of intergovernmental organisation*s. Available at: https://www.unodc.org/documents/treaties/organized_crime/COP5/CTOC_COP_2010_CRP7x/CTOC_COP_2010_CRP7x.pdf (accessed on: 28 December 2019).

Urquhart, C. 2013. *Grounded theory for qualitative research: A practical guide*. Los Angeles: Sage.

Van Cleave, M. 2009. Strategic counterintelligence: What it is and what should we do about it? (15-36). In J.M. Deady. (Ed.). *21st Century counterintelligence*. New York: Nova Science.

Vansteenkiste, M., Ryan, R.M. & Soenens, B. 2020. Basic psychological need theory: Advancements, critical themes, and future directions. *Motivation and Emotion,* 44:1-31.

Vise, D.A. 2002. *From Russia with love.* Available at: https://www.washingtonpost.com/archive/lifestyle/magazine/2002/01/06/from-russia-with-love/b28c2127-65e5-43f3-8a9a-0e75ab851cb3/?utm_term=.218050a050e7 (accessed on: 05 May 2017).

Walker, L. 2022. *EU calls on Belgium to strengthen anti-espionage efforts*. Available at: https://www.brusselstimes.com/210379/eu-calls-on-belgium-to-strengthen-anti-espionage-efforts (accessed on: 26 March 2022).

Wallace, R. & Melton, H.K. 2008. *Spycraft*. London: Penguin.

Warner, M. 2007. Sources and methods of the study of intelligence (17-27). In L.K. Johnson. (Ed.). *Handbook of intelligence studies*. London: Routledge.

Wąsiński, J. 2015. Information and communication technologies in the management systems of small businesses. (53-78). In J. Kowal, M. Wawrzak-Chodaczek & H. Żeligowski. (Eds). *Communication and information technology in society: Volume 2: Information and communication technologies (ICT) in management*. Newcastle upon Tyne: Cambridge Scholars.

Webster, S.W. 2018. It’s personal: The big five personality traits and negative partisan affect in polarized U.S. politics. *The American Behavioural scientist,* 62(1):127-145.

Weston, G. 2013. *Snowden document shows Canada set up spy posts for NSA.* Available at: https://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886 (accessed on: 27 April 2022).

Weiser, B. 2004. *A secret life*. New York: Public Affairs.

Wilson, J. 2014. *Essentials of business research. A guide to doing research.* Sage: London.

Wilder, U.M. 2017. The psychology of espionage. *Studies in Intelligence,* 61(2):19-36.

Wimmer, B. 2015. *Business espionage: Risks, threats, and countermeasures*. Waltham: Butterworth Heinemann.

Wyden, R. 2013. *DNI Clapper tells Wyden the NSA does not collect data on millions of Americans.* Available at: https://www.youtube.com/watch?v=QwiUVUJmGjs&t=426s (accessed on: 27 April 2022).

Yin, R.K. 2018. *Case study research: Design and methods*. Thousand Oaks: Sage.

Zuckerman, M. 1994. *Behavioral expressions and biosocial bases of sensation seeking*. Cambridge: Cambridge University Press.

Zuckerman, M., Kuhlman, D.M., Joireman, J., Teta, P. & Kraft, M. 1993. A comparison of three structural models for personality: The big three, the big five, and the alternative five. *Journal of Personality and Social Psychology,* 65(4):757-768.

Zuckerman, M., Kuhlman, D.M., Thornquist, M. & Kiers, H.A.L. 1991. Five (or three) Robust questionnaire scale factors of personality without culture. *Personality and Individual Differences,* 12(9):929-941.

ANNEXURES

8.1 ANNEXURE A: LIST OF ESPIONAGE CASES

1. Abujihaad, Hassan
2. Ahadi, (pseudonym)
3. Allen, Michael Hahn
4. Alonso, Alejandro M.
5. Alvarez, Carlos
6. Abujihaad, Hassan
7. Ahadi, (pseudonym)
8. Allen, Michael Hahn
9. Alonso, Alejandro M.
10. Alvarez, Carlos
11. Alvarez, Elsa
12. Ames, Aldrich Hazen
13. Ames, Maria del Rosario
14. Anderson, Ryan Gibson
15. Anzalone, Charles Lee
16. Aragoncillo, Leandro
17. Baba, Stephen Anthony
18. Barczatis, Elli
19. Barnett, David Henry
20. Barr, Joel
21. Baynes, Virginia Jean
22. Bell, William Holden
23. Bergling, Stig
24. Betzing, Lorenz
25. Blake, George
26. Baumann, Winfried
27. Blau, Hagen
28. Blunt, Anthony 'Johnson'
29. Boeckenhaupt, Herbert William
30. Boone, David Sheldon
31. Borger, Harold Noah
32. Borm, William
33. Boyce, Christopher John
34. Bronson, (pseudonym)
35. Brown, Joseph Garfield
36. Brown, Russell Paul
37. Buchanan, Edward Owen
38. Burgess, Guy 'Hicks'
39. Butenko, John William
40. Cairncross, John 'Liszt'
41. Carney, Jeffrey M
42. Cascio, Guiseppe
43. Cavanagh, Thomas Patrick
44. Charlton, John Douglas
45. Chin, Larry Wu-Tai
46. Chiu, Rebecca Laiwah
81. Haeger, John Joseph
82. Haguewood, Robert Dean
83. Hall, James William
84. Hamilton, Frederick Christopher
85. Hamilton, Victor Norris
86. Hanssen, Robert Philip
87. Harper, James Durward, Jr.
88. Harris, Ulysses Leonard
89. Hauffe, Karl
90. Hawkins, Stephen Dwayne
91. Heilmann, Peter
92. Helmich, Joseph George
93. Hernandez, Linda
94. Hernandez, Nilo
95. Hoffman, Ronald Joshua
96. Horton, Brian Patrick
97. Humphrey, Ronald Louis
98. Irene, Dale Vern
99. Jeffries, Randy Miles
100. Jenott, Eric O.
101. Johnson, Robert Lee
102. Jones, Geneva
103. Kampiles, William Peter
104. Kauffman, Joseph Patrick
105. Keyser, Donald Willis
106. Kim, Robert Chaegon
107. King, Donald Wayne
108. Koecher, Karel Frantisek
109. Kota, Subrahmanyam
110. Koval, George
111. Kunkle, Craig Dee
112. Kuron, Klaus
113. Lalas, Steven J.
114. Ledbetter, Gary Lee
115. Lee, Andrew Daulton
116. Lee, Peter H.
117. Lessenthien, Kurt G.
118. Leung, Katrina M.
119. Lipka, Robert Stephan
120. Löffler, Gerd
121. Lonetree, Clayton John
122. Lorenzen, Ursula
148. Pickering, Jeffrey Loring
149. Pizzo, Francis Xavier
150. Pollard, Anne, Henderson
151. Pollard, Jonathan Jay
152. Polyakov, Dmitri
153. Ponger, Kurt Leopold
154. Prellwitz, Wolf-Heinrich
155. Ramsay, Roderick James
156. Rees, Norman john
157. Regan, Brian Patrick
158. Reißmann (aka, Ursula, Richter'), Erika
159. Rhodes, Roy Adair
160. Richardson, Daniel Walter
161. Rohrer, Glenn Roy
162. Rondeau, Jeffrey Stephen
163. Safford, Leonard Jenkins
164. Santos, Joseph
165. Sarant, Alfred
166. Sattler, James Frederick
167. Scarbeck, Irvin Chambers
168. Schlicht, Götz
169. Schmidt-Wittmack, Karlfranz
170. Schoof, Charles Edward
171. Schuler, Ruby Louise
172. Schwartz, Michael Stephen
173. Scranage, Sharon Marie
174. Seldon, Phillip Tyler
175. Shaaban, Shaaban Hafed
176. Simm, Herman
177. Skripal, Sergei Wiktorowitsch
178. Slatten, Charles Dale
179. Slavens, Brian Everett
180. Smith, Richard Craig
181. Sombolay, Albert T.
182. Snowden, Edward
183. Squillacote, Theresa M.
184. Stiller, Werner
185. Szabo, Zoltan

47. Clark, James
48. Conrad, Clyde Lee
49. Cooke, Christopher M.
50. Cordrey, Robert Ernest
51. Cremer, Friedrich
52. Davies, Allen John
53. DeChamplain, Raymond George
54. Dedeyan, Sahag Katcher
55. Delisle, Jeffrey Paul
56. Dolce, Thomas Joseph
57. Donhauser, Anton
58. Dressen, Aleksei
59. Drummond, Nelson C.
60. Dubberstein, Waldo Herman
61. Dunlap, Jack Edward
62. Ellis, Robert Wade
63. Faget, Mariano
64. Faris, Iyman
65. Felfe, Heinz
66. Feuerstein, Dieter
67. Ford, Kenneth Wayne
68. Franklin, Lawrence Anthony
69. French, George Holmes
70. Frenzel[], Alfred
71. Garcia, Wilfredo
72. Gessner, George John
73. Gilbert, Otto Attila
74. Gordijewski, Oleg
75. Graf, Ronald Dean
76. Gregory, Jeffery Eugene
77. Groat, Douglas Frederick
78. Grunden, Oliver Everett
79. Grunert, Rolf
80. Guerrero, Antonio

123. MacLean, Donald 'Homer'
124. Madsen, Lee Eugene
125. Mak, Chi
126. Manning, Chelsea
127. Martin, William Hamilton
128. Marwan, Ashraf
129. Mehalba, Ahmed
Miller, Richard
130. Miller, Richard William
131. Mintkenbaugh, James Allen
132. Mira, Francisco de Asis
133. Mitchell, Bernon Ferguson
134. Mohamed, Ali Abdelseoud
135. Montaperto, Ronald N.
136. Montes, Ana Belen
137. Moore, Edwin Gibbons
138. Morison, Samuel Loring
139. Mortati, Thomas
140. Ott, Bruce Damian
141. Payne, Leslie Joseph
142. Pelton, Ronald William
143. Penkovskiy, Oleg 'Hero'
144. Peri, Michael Anthony
145. Perkins, Walter Thomas
146. Petersen, Joseph Sidney, Jr.
147. Philby, Kim 'Stanley'

186. Teske, Werner
187. Thompson, Robert Glenn
188. Tobias, Michael Timothy
189. Tomberg, Friedrich
190. Trofimoff, George
191. Tsou, Douglas S.
192. Tumanova, Svetlana
193. Veitman, Vladimir
194. Verber, Otto
195. von Raussendorff, Klaus
196. Walker, Arthur James
197. Walker, John Anthony
198. Walker, Michael Lance
199. Walter Biot
200. Walton, (pseudonym)
201. Warren, Kelly Therese
202. Weinmann., Ariel Jonathan
203. Weirauch, Lothar
204. Wesson, (pseudonym)
205. Whalen, William Henry
206. Whitworth, Jerry Alfred
207. Wienand, Karl
208. Willner, Astrid
209. Wilmoth, James Rodney
210. Wine, Edward Hilledon
211. Winzer, Bruno
212. Wold, Hans Palmer
213. Wolf, Ronald Craig
214. Wolff, Jay Clyde
215. Wood, James David
216. Yai, John Joungwoong
217. Lüneburg), Johanna

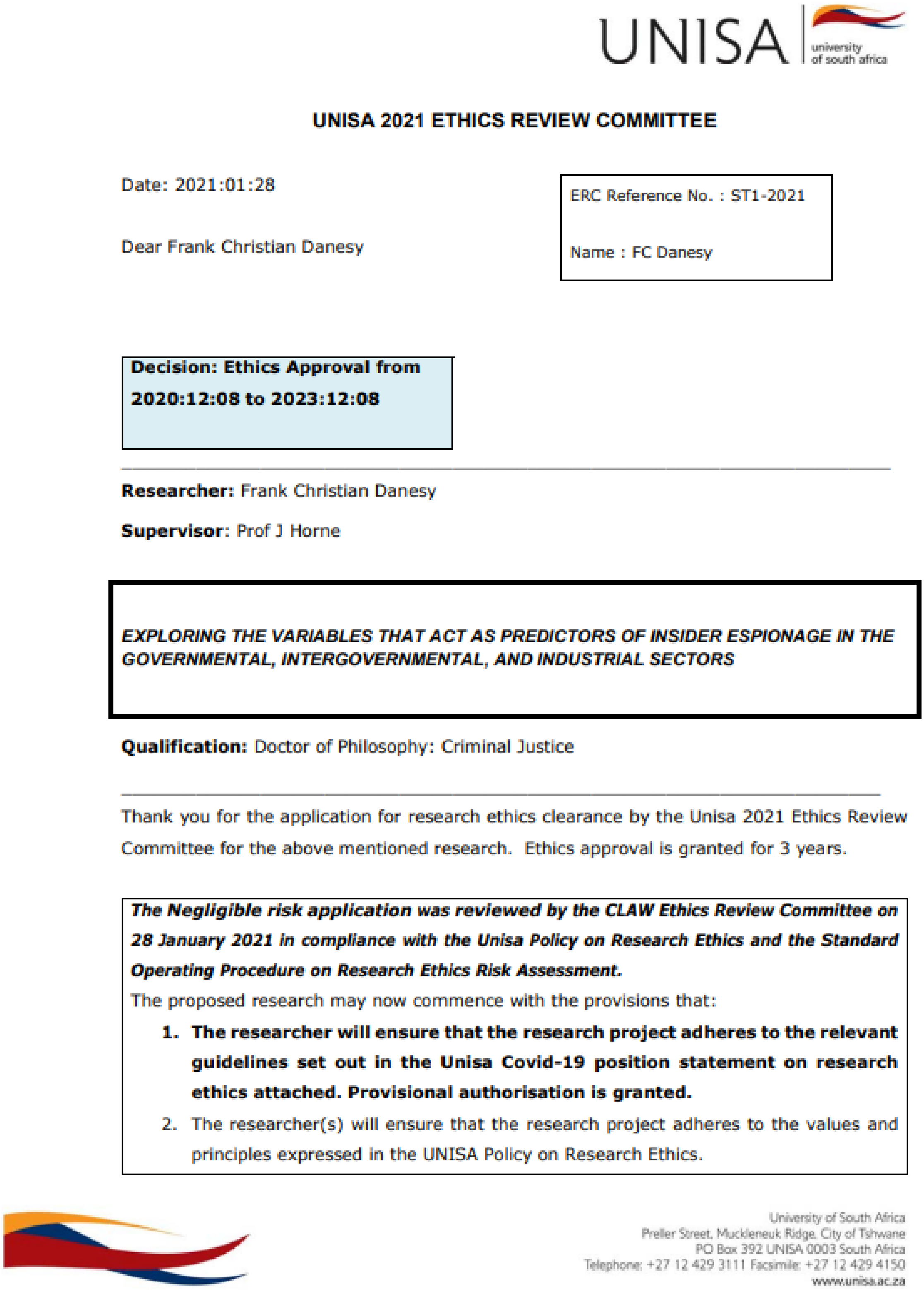
8.2 ANNEXURE B: CODES AND CODE DEFINITIONS

Code	Definition
1. **Triggers**	A trigger is an event or situation that initiates motivation processes (Keltner & Shiota, 2003:89; Deckers, 2016:33).
1.1 **Stimulus**	An event or situation that elicits a reaction (American Psychological Association, 2020).
1.2 **Predisposition**	Tendency to hold a particular attitude or act in a particular way with respect to needs, beliefs, values, and ideologies ideology (Deckers, 2016:369; McClelland, 1987:6; Rokeach,1968:113).
1.3 **Need**	A need is a predisposition 'that is essential for an individuals' adjustment, integrity, and growth' (Vansteenkiste et al., 2020:1).
1.4 **Belief**	Beliefs are key elements and play a central role in our cognitive processes because they reflect what we think is true or not (McClelland, 1987:518-519; Cottam et al., 2010:131-132).
1.5 **Value**	Prescriptive beliefs that are global and unspecific with respect to an object or situation are referred to as values (Cottam et al., 2010:132).
1.6 **Ideology**	Ideology is an organisation of religious, political, or philosophical beliefs that are 'more or less institutionalized or shared with others' (Rokeach, 1968:123-124).
2. **Motivation process**	A motivation process is a sequence that is initiated by a trigger and involves (a) the appraisal of the trigger, (b) an emotional response to the trigger based on the appraisal, and (c) some level of action readiness based on the emotional response (Deckers, 2016:369).
2.1 **Appraisal**	Appraisal is an intervening process that follows the emotion- eliciting event or situation and precedes the emotional response to the event or situation. It determines the emotional response to the event or situation (Roseman & Smith, 2001:3).
2.2 **Emotion**	An emotion is a 'universal, functional reaction to an external stimulus event, temporarily integrating physiological, cognitive, phenomenological, and behavioural channels to facilitate a fitness-enhancing, environment-shaping response to the current situation' (Keltner & Shiota, 2003:89).
2.3 **Anger**	Anger is an emotion that results from events and situations which threaten or thwart an individual's goals by bringing about outcomes that the individual considers negative (Angie et al., 2011:1395 & 1414).
2.4 **Happiness**	Happiness is an emotion associated with feelings of elation and light-heartedness (Tiedens & Linton, 2001:973).
2.5 **Fear**	Fear is a 'sense of impending evil' that results from the perception of a threat, uncertainty about the threat, and uncertainty about one's own ability to cope with the threat (Frijda, 1986:74 & 197).
2.6 **Sadness**	Sadness is an emotion that is associated with emptiness or barrenness and 'the explicit absence of something valued' (Frijda, 2010:199).
2.7 **Action Readiness**	Action readiness refers to the individual's wish to act on a given emotion so as to fulfil the aim of the emotion (Deckers, 2016:47).

2.8 Motive	A motive is a need, belief, value, or ideology that is activated (triggered) by events or situations and that pushes the individual to some form of action (Maslow, 1970/1987:60-63; Deckers 2016:369-370).
3. Situational Vulnerability	A vulnerability is an ‘exploitable condition in which the adversary has sufficient knowledge, time and available resources to thwart friendly mission accomplishment or substantially increase operational risk’ (Secretary of the Air Force, 2020:59).
3.1 Information Vulnerability	A vulnerability related to the way an organisation handles its information (Secretary of the Air Force, 2020:59).
3.2 Cyber/ Communications Vulnerability	A vulnerability related to the way an organisation handles its information technology and communications (Secretary of the Air Force, 2020:59).
3.3 Physical Vulnerability	A vulnerability related to the way an organisation handles its physical layout (Secretary of the Air Force, 2020:59).
3.4 Personnel Vulnerability	A vulnerability related to the way an organisation screens its personnel (Secretary of the Air Force, 2020:59).
4. Market	A market is a system that brings together ‘the forces of supply and demand for a particular good or service’ and that consists of customers, suppliers, and mechanisms for effecting transactions (Imber & Toffler, 2000:342).
4.1 Supplier	The provider of a good or service (Imber & Toffler, 2000:342)
4.2 Customer	The recipient of of a good or service (Imber & Toffler, 2000:342)
4.3 Information	A type of good or services provided by the supplier in a market transaction (Imber & Toffler, 2000:342)
4.4 Incentive	A benefit that the supplier expects to receive from the market transaction (Imber & Toffler, 2000:342)
5. Disinhibiting Factors	Disinhibiting factors are factors that causes an individual’s inclination to comply with social norms to erode. These factors may be 1) emotional reactions, 2) personality structure, and 3) mental disorders (Keltner & Shiota, 2003:89; Deckers, 2016:41-47 & 359, American Psychiatric Association, 2013:20).
5.1 Decision	A decision is ‘a commitment to a course of action (Newell et al., 2015:20).
5.2 Emotion	An emotion is a ‘universal, functional reaction to an external stimulus event, temporarily integrating physiological, cognitive, phenomenological, and behavioral channels to facilitate a fitness-enhancing, environment-shaping response to the current situation’ (Keltner & Shiota, 2003:89). (See above).
5.3 Personality Structure	Personality structure is the enduring configuration of characteristics and behaviour defined by five dimensions:1) neuroticism, 2) extraversion, 3) openness, 4) ‘agreeableness’, and 5) conscientiousness (Barrick & Mount, 1991:849; Costa & McCrae, 1985:1; Digman, 1990:417; Gross, 2019:723).

5.4 Mental Disorder	A mental disorder as ‘a syndrome characterized by clinically significant disturbance in an individual's cognition, emotion regulation, or behavior that reflects a dysfunction in the psychological, biological, or developmental processes underlying mental functioning’ (American Psychiatric Association, 2013:20).
5.5 Bipolar Disorder	A disorder in which affected individuals experience both, manic and depressive episodes (American Psychiatric Association,2013:123-124).
5.6 Personality Disorder	A personality disorder is defined as an ‘[enduring pattern of inner experience and behavior that deviates markedly from the expectations of the individual’s culture, is pervasive and inflexible, and has an onset in adolescence or early adulthood, is stable over time, it leads to distress or impairment’ (American Psychiatric Association, 2013:645).
5.7 Substance-related and addictive disorder	Substance-related and addictive disorders encompass a variety of substances (i.e. alcohol, caffeine, cannabis, hallucinogens, inhalants, opioids, sedatives, stimulants, and tobacco) as well as gambling (American Psychiatric Association, 2013:482 & 585)

8.3 ANNEXURE C: UNISA ETHICAL CLEARANCE



UNISA university of south africa

UNISA 2021 ETHICS REVIEW COMMITTEE

Date: 2021:01:28

Dear Frank Christian Danesy

ERC Reference No. : ST1-2021

Name : FC Danesy

Decision: Ethics Approval from 2020:12:08 to 2023:12:08

Researcher: Frank Christian Danesy

Supervisor: Prof J Horne

EXPLORING THE VARIABLES THAT ACT AS PREDICTORS OF INSIDER ESPIONAGE IN THE GOVERNMENTAL, INTERGOVERNMENTAL, AND INDUSTRIAL SECTORS

Qualification: Doctor of Philosophy: Criminal Justice

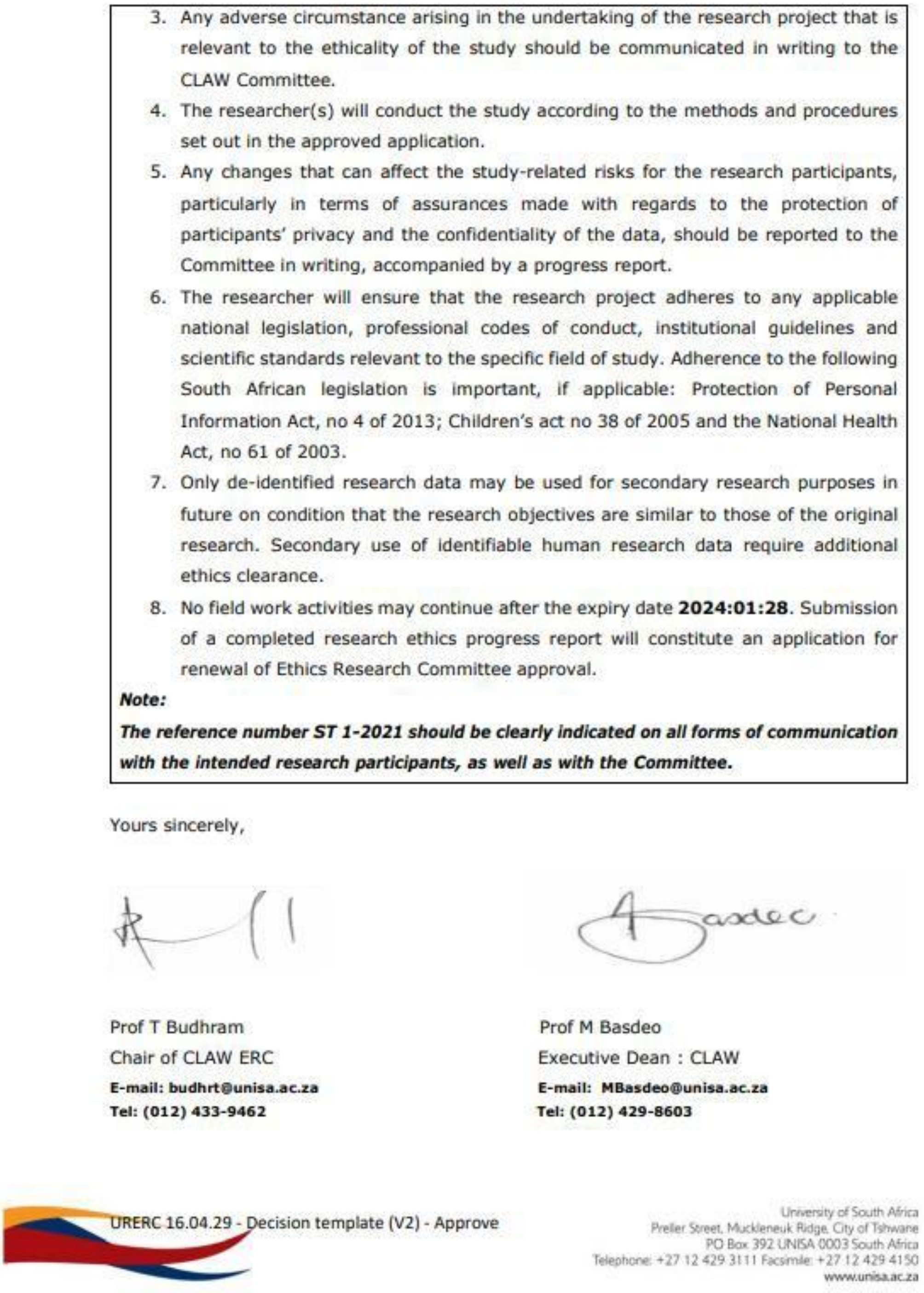
Thank you for the application for research ethics clearance by the Unisa 2021 Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

The Negligible risk application was reviewed by the CLAW Ethics Review Committee on 28 January 2021 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.

The proposed research may now commence with the provisions that:

1. **The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached. Provisional authorisation is granted.**
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date **2024:01:28**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number ST 1-2021 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

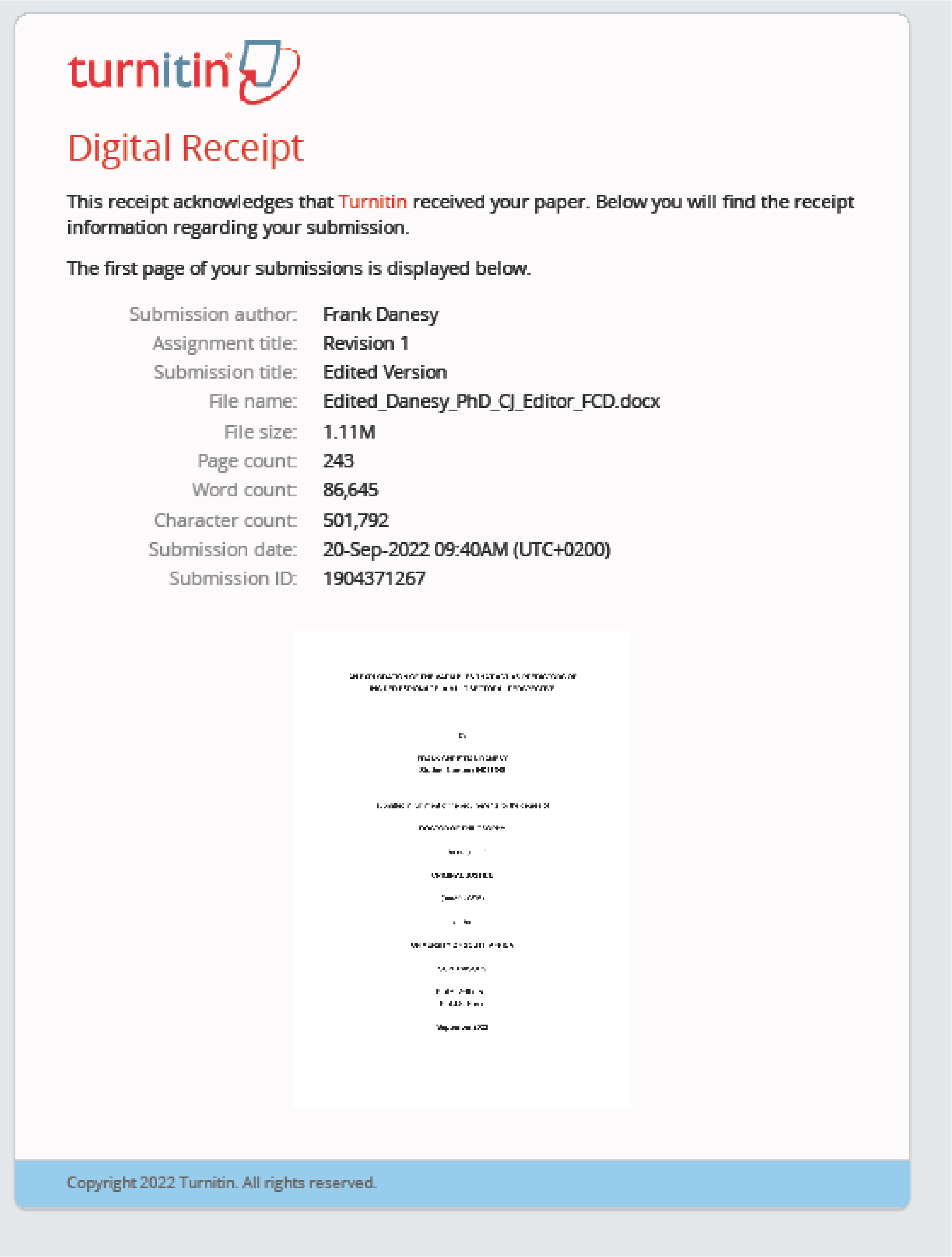
Prof T Budhram
Chair of CLAW ERC
E-mail: budhrt@unisa.ac.za
Tel: (012) 433-9462

Prof M Basdeo
Executive Dean : CLAW
E-mail: MBasdeo@unisa.ac.za
Tel: (012) 429-8603

URERC 16.04.29 - Decision template (V2) - Approve

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

8.4 ANNEXURE D: TURNITIN DIGITAL RECEIPT



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:	Frank Danesy
Assignment title:	Revision 1
Submission title:	Edited Version
File name:	Edited_Danesy_PhD_CJ_Editor_FCD.docx
File size:	1.11M
Page count:	243
Word count:	86,645
Character count:	501,792
Submission date:	20-Sep-2022 09:40AM (UTC+0200)
Submission ID:	1904371267

8.5 ANNEXURE E: EDITOR’S LETTER

I, the undersigned, hereby confirm my involvement in the language editing, text redaction, checking for the research methodology compatibility and technical compliance regatrding the research manuscript of **Dr Frank Chrisitian Danesy (Student Number: 64011348)** in respect of his fulfilment of the requirement for his Doctor of Philosophy (PhD) in Criminal Justice degree registered with the University of South Africa (UNISA), and entitled:

An exploration of the variables that act as predictors of insider espionage: A multisectoral perspective

As an independent academic editor, I attest that all possible means have been expended to ensure the final draft of **Dr F.C. Danesy’s** thesis manuscript reflects both acceptable research methodology practices and language control standards expected of postgraduate research studies at his academic level.

In compliance with conventional ethical requirements in research, I have further undertaken to keep all aspects of **Dr F.C.’s** research study confidential, and as his own individual initiative.

Sincerely.

TJ Mkhonto
BA Ed: North-West University, Mafikeng (1985)
MEd: School Administration; University of Massachusetts-at-Boston, USA, Harbor Campus (1987)
DTech: Higher Education Curriculum Policy Reform, Design & Management; University of Johannesburg, (2008)

All enquiries:

Email: mkhonto9039@gmail.com
Cell: +27(0)60 401 8279

Signed: ________________________ **Date:** 15 September 2022

Dr T.J. Mkhonto dd/mm/yyyy

Independent Academic Editor

Professional EDITORS Guild

Themba J Mkhonto
Associate Member

Membership number: MKH001
Membership year: February 2022 to March 2023

060 401 8279
mkhonto9039@gmail.com

www.editors.org.za