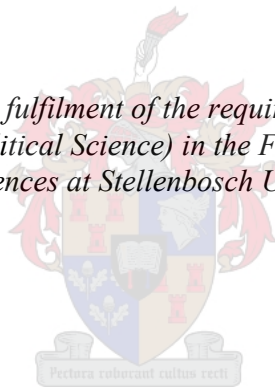


# **Cyber-threats as Political Risk: Increased Risk for the Oil and Gas Industry**

by  
Kayla Ann Mc Ewan

*Thesis presented in fulfilment of the requirements for the degree of  
Master of Arts (Political Science) in the Faculty of Arts and Social  
Sciences at Stellenbosch University*



Supervisor: Dr Derica Lambrechts

March 2020

## **Declaration**

By submitting this thesis/dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously, in its entirety or in part, submitted it for obtaining any qualification.

Date: March 2020

## **Abstract**

The oil and gas industry has always had a high vulnerability to risk, despite the high risk associated with the industry companies continue to invest in the industry because of the potential high profit return. Traditionally one of the biggest risks facing oil and gas companies is the political risk of terrorism. Since the early 1990s international oil and gas companies have been the target of terrorist groups with the number of attacks increasing yearly. The advent of the Internet and the rapid development and advancement of technology has brought with it a new political risk: cyber-threats. In comparison to terrorist attacks on oil and gas companies, cyber-threats are more of a recent phenomenon with cyber-attacks only starting to be documented over the last ten years. Two of the most well-documented cases of cyber-attacks on oil and gas companies were the 2012 attack on Saudi Aramco and the 2014 attack on Norwegian oil and gas companies. These two cyber-attacks resulted in greater attention being paid to the risk of cyber-threats facing the oil and gas industry and their overall influence. This study argues that while cyber-threats are a more recent phenomenon, they are already having a noticeable influence on international oil and gas companies. Cyber-attacks are starting to occur more frequently and increasing the political risk faced by international oil and gas companies, as well as forcing them to change the way that they think and do risk mitigation and management. As such, the main research question informing this study seeks to determine whether or not cyber-threats increase the political risk which oil and gas companies face; it specifically analyses the Shamoon attack on Saudi Aramco and the cyber-attack on Statoil and other Norwegian oil and gas companies. The aim of this study is to answer this question along with three others, which complement and support the main research question. The first sub-question concerns which vulnerabilities of cyber-threats can be identified and used by companies in the oil and gas industry in order to help them manage and/or mitigate the risk of cyber-threats. The second looks at whether cyber-attacks will result in oil and gas companies losing revenue and halt their operations. The third sub-question looks at the possibilities of international oil and gas companies mitigating the risk of cyber-threats, or whether cyber-threats are a risk that can only be managed. Findings suggest that cyber-attacks are increasing the political risk faced by international oil and gas companies in various ways and they will need to change the way they approach risk management in order minimize the impact of cyber-threats.

## Opsomming

Die olie- en gasindustrie was nog altyd baie vatbaar vir risiko's. En tog, ten spyte van die hoë risiko's wat met die industrie geassosieer word, gaan maatskappye voort om in die industrie te investeer omrede die potensiële hoë winsopbrengs. Tradisioneel is terrorisme een van die grootste politieke bedreigings in die olie- en gasbedryf. Sedert die vroeë 1990's word internasionale olie- en gasmaatskappye deur terroriste groepe geteiken en was daar jaarliks 'n toename in die aantal aanvalle. Die koms van die Internet en die vinnige ontwikkeling en vooruitgang van tegnologie het 'n nuwe politieke risiko, nl. kuberbedreigings meegebring. In vergelyking met terroriste aanvalle op olie- en gasmaatskappye, is kuberaanvalle 'n meer onlangse verskysel wat eers gedurende die afgelope tien jaar gedokumenteer word. Twee van die mees gedokumenteerde gevalle van aanvalle op olie- en gasmaatskappye, is die aanval op Saudi Aramco in 2012 en die aanval op 'n Noorweegse olie- en gasmaatskappy in 2014. Hierdie twee kuberaanvalle het daartoe gelei dat meer aandag gegee word aan die risiko van kuberbedreigings wat die olie- en gasbedryf in die gesig staar, asook die omvattende impak daarvan. Die uitgangspunt van hierdie studie is dat ten spyte daarvan dat kuberbedreigings 'n baie onlangse neiging is, dit reeds 'n beduidende impak op internasionale olie- en gasmaatskappye het. Kuberaanvalle vind al meer gereeld plaas en verhoog die politieke risiko wat deur internasionale olie- en gasmaatskappye ervaar word. Verder dwing dit die maatskappye om hulle denkwysse te verander en, risiko's te verminder en te bestuur. Vervolgens is die primêre navorsingsvraag van die studie om te bepaal of kuberbedreigings die politieke risiko wat olie- en gasmaatskappye in die gesig staar, toeneem al dan nie. Die studie analiseer spesifiek die Shamoon aanval op Saudi Aramco en die kuberaanval op Statoil en ander Noorweegse olie- en gasmaatskappye. Die doel van die studie is om hierdie vraag in ooreenstemming met drie ander aanvullende en ondersteunende vrae te beantwoord. Die eerste subvraag het betrekking op watter kwesbaarhede in die kuberaanvalle geïdentifiseer en gebruik kan word deur die maatskappy om sodoende 'n bydrae te lewer tot die bestuur en/of vermindering van die risiko wat kuberbedreigings inhou. Die tweede vraag is gerig op die moontlikheid dat kuberaanvalle op die maatskappy sal lei tot 'n verlies aan inkomste of selfs die staking van produksie. Die derde vraag ondersoek die moontlikhede dat internasionale olie- en gasmaatskappye die risiko van kuberaanvalle verminder, of indien daar 'n risiko van kuberaanvalle bestaan, dit bloot bestuur kan word. Volgens bevindinge verhoog kuberaanvalle die politieke risiko wat die internasionale olie- en gasmaatskappye in die gesig staar op verskeie maniere en maatskappye sal die wyse waarop hulle risikobestuur benader ten eide die aanslag van kuberbedreigings te verminder.

## **Acknowledgements**

In all honesty, there were times throughout the past two years when I was writing this thesis when the writing of these acknowledgements was a far-off unattainable reality. I looked forward to this moment because I thought that in comparison to all the other writing this would be a breeze and yet here I am; and I have no idea what to write.

Firstly, I need to say a massive thank you to my supervisor, Dr Derica Lambrechts. Thank you for all your advice, encouragement, consistency, wisdom and support throughout the last two years. You have invested a lot of time and effort into this thesis which has helped me continually improve and be better. I am truly beyond grateful to have been given the opportunity to have worked with you. I could not have asked for a better advisor than you.

To my phenomenal parents Butch and Lesa. Thank you for your endless support, encouragements and reminders to take a deep breath and telling me I can do this during days when I truly believed I couldn't. As well as for listening to me ramble on about bits and pieces of this thesis that I could not get my head around and put on paper and for giving me a different perspective that always helped. Thank you for all the sacrifices you have made for me in the past that have made this possible - without the two of you none of this would have been possible and this is as much your success as it is mine.

To my sister Megan, who despite being younger than me continually inspires me through her hard work and determination. Meg, you were my provider of food on days I couldn't be bothered and for always helping me forget about my stress with a good laugh.

Thank you to my grandparents Bruce and Jennifer, who understood the importance of my education when I started my undergraduate degree. Without your support I would not have been able to reach the stage of writing a master's thesis.

Lastly, I need to thank the van Dyk family (Hennie, Christine, Philip and Tristan) who were an incredible support to me by having me as a guest when I needed a change of environment and being there to remind me to celebrate all the little moments.

## List of Tables and Figures

Table 1: Cyber-Threats: Defining Terms.....	42
Table 2: Top Ten Vulnerabilities to Cyber-threats in the Oil and Gas Industry.....	74
Figure 1: Cyber-threats faced by the oil and gas sector as compared to all industrial sectors .....	52
Figure 2: Flow of the operations in the Oil and Gas Industry .....	54
Figure 3: Cyber vulnerability/severity matrix of upstream operations.....	56
Figure 4: Cyber vulnerability/severity matrix of downstream operations .....	68

## Acronyms

AIS	Marine Automatic Systems
BMS	Burner Management system
BP	British Petroleum
DCS	Distributed control systems
DDos	Denial of Service
DOD	Department of Defense
ECDIS	Electronic Chart Display
ENISA	European Union Agency for Network and Information Security
ERP	People's Revolutionary Army
FATs	Functional acceptance tests
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
ICS	Industrial control system
ICT	Information and Communication Technology
IMF	International Monetary Fund
IoT	Internet of Things
IPO	Initial public offering
ISP	Internet service provider
IT	Information Technology
ITERATE	The International Terrorism: Attributes of Terrorist Events
ITU	International Telecommunication Union
MES	Manufacturing Execution Systems
MNC	Multinational Corporation
NSM	Nasjonal Sikkerhetsmyndighet
OPC	Open Platform Communications
OPEC	Organisation of Arab Petroleum Exporting Countries
OT	Operational Technology
PKK	Kurdistan Workers' Party
PLC	Programable Logical Controllers
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition

SIS	Safety Instrumented System
SOC	Security Operation Centre
TIA	Tank Inventory System
US	United States of America



## Table of Contents

<b>DECLARATION</b> .....	<b>I</b>
<b>ABSTRACT</b> .....	<b>II</b>
<b>OPSOMMING</b> .....	<b>III</b>
<b>ACKNOWLEDGEMENTS</b> .....	<b>IV</b>
<b>LIST OF TABLES AND FIGURES</b> .....	<b>V</b>
<b>ACRONYMS</b> .....	<b>VI</b>
<b>CHAPTER ONE: INTRODUCTION</b> .....	<b>1</b>
1.1 BACKGROUND TO THE RESEARCH STUDY.....	1
1.2 PRELIMINARY LITERATURE REVIEW .....	6
1.3 RESEARCH PROBLEM AND RESEARCH QUESTION.....	8
1.4 OBJECTIVE AND RELEVANCE OF THE RESEARCH STUDY.....	11
1.5 RESEARCH DESIGN AND RESEARCH METHODOLOGY .....	12
1.6 LIMITATION OF RESEARCH STUDY .....	14
1.7 OUTLINE OF THE RESEARCH STUDY.....	15
1.8 CONCLUSION .....	16
<b>CHAPTER TWO: THEORETICAL PERSPECTIVE AND CONTEXTUALISATION</b> .....	<b>18</b>
2.1 INTRODUCTION .....	18
2.2 RATIONAL CHOICE THEORY, PROBLEM-SOLVING AND DECISION-MAKING THEORY: A THEORETICAL GROUNDING.....	19
2.3 RISK.....	22
2.4 POLITICAL RISK.....	24
2.5 MACRO AND MICRO POLITICAL RISK.....	30
2.6 RISK MANAGEMENT AND RISK MITIGATION .....	34
2.7 CYBER-THREATS.....	36
2.7.1 CYBER-ATTACKS .....	43
2.10 CONCLUSION.....	47
<b>CHAPTER THREE: IDENTIFYING VULNERABILITIES TO CYBER-THREATS IN THE OIL AND GAS INDUSTRY</b> .....	<b>49</b>
3.1 INTRODUCTION .....	49
3.2 AUTOMATION AND THE INTERNET OF THINGS (IoT) IN THE OIL AND GAS INDUSTRY.....	49
3.3 OVERVIEW OF CYBER-THREATS TO THE UPSTREAM SECTOR OF THE OIL AND GAS INDUSTRY .....	54
3.3.1 <i>Identifying Cyber-threat Vulnerabilities in the Exploration stage</i> .....	56
3.3.2 <i>Identifying Cyber-threat Vulnerabilities in the Development stage</i> .....	59
3.3.3 <i>Identifying Cyber-threat Vulnerabilities in the Production stage</i> .....	61

3.4 OVERVIEW OF CYBER-THREATS TO THE MIDSTREAM SECTOR OF THE OIL AND GAS INDUSTRY .....	62
3.4.1 <i>Identifying Cyber-threat Vulnerabilities in the Distribution Sector</i> .....	63
3.5 OVERVIEW OF CYBER-THREATS TO THE DOWNSTREAM SECTOR OF THE OIL AND GAS INDUSTRY .....	66
3.5.1 <i>Identifying Cyber-threat Vulnerabilities in the Processing and Refining Sector</i> .....	69
3.5.2 <i>Identifying Cyber-threat Vulnerabilities to the Trading sector</i> .....	71
3.6 VULNERABILITIES TO CYBER-THREATS IDENTIFIED WITHIN THE OIL AND GAS INDUSTRY .....	73
VULNERABILITY .....	74
EXPLANATION OF VULNERABILITY .....	74
3.7 CONCLUSION .....	76
<b>CHAPTER FOUR: THE INFLUENCE OF CYBER-THREATS ON THE OIL AND GAS INDUSTRY... 78</b>	
4.1 INTRODUCTION .....	78
4.2 CYBER ATTACK ON OIL AND GAS COMPANIES IN SAUDI ARABIA .....	78
4.2.1 <i>Events Prior to Shamoan Attack</i> .....	79
4.2.2 <i>Saudi Aramaco’s Cyber-security prior to Shamoan attack</i> .....	82
4.2.3 <i>Outline of the events of the Shamoan attack on Saudi Aramco</i> .....	84
4.2.4 <i>Further investigation of the Shamoan attack on Saudi Aramco</i> .....	87
4.2.5 <i>Legacy of Shamoan Attack on Saudi Aramco</i> .....	91
4.2.6 <i>Second Cyber-attack on a Saudi Aramco Petrochemical plant</i> .....	92
4.2.7 <i>Evaluating the Presence of Vulnerabilities to Cyber-threats in the Saudi Aramco Case Study</i> .....	96
4.3 CYBER-ATTACK ON OIL AND GAS COMPANIES IN NORWAY.....	97
4.3.1 <i>Statoil cyber-security prior to the 2014 cyber-attack on Norwegian oil and gas companies</i> .....	98
4.3.2 <i>Outline of the Events of the Cyber-attack on Oil and Gas Companies in Norway</i> .....	100
4.3.3 <i>Further Investigation and Findings of the Norwegian Cyber-attack</i> .....	101
4.3.4 <i>Legacy of cyber-attack on Oil and Gas Companies in Norway</i> .....	105
4.3.5 <i>Evaluating the Presence of Vulnerabilities to Cyber-threats in the Norwegian Case Study</i> .....	106
4.4 THE MANAGEMENT OF CYBER-THREATS AND COMPLICATIONS WITH MITIGATION.....	107
4.5 RISK MANAGEMENT RECOMMENDATIONS FOR THE OIL AND GAS INDUSTRY .....	109
4.6 CONCLUSION .....	110
<b>CHAPTER FIVE: CONCLUSION AND EVALUATION OF THE RESEARCH STUDY ..... 112</b>	
5.1 INTRODUCTION .....	112
5.2 PROGRESS OF THE RESEARCH STUDY .....	113
5.3 MAIN FINDINGS OF THE RESEARCH .....	114
5.4 EVALUATION OF THE RESEARCH STUDY .....	117
5.5 RECOMMENDATION OF FURTHER RESEARCH.....	118
5.6 CONCLUSION .....	120

**BIBLIOGRAPHY ..... 121**

## Chapter One: Introduction

### 1.1 Background to the Research Study

Political risk is a concept that first began to emerge during the 1970s.<sup>1</sup> For a long-time political risk was predominantly associated with its application to an investing company and the host government of a country, in which the company was seeking to invest. In this instance it was only select groups, majority groups and foreign business operations and investments that were negatively impacted by a government's policies or societies' actions (Simon, 1982:68). Political risk analysis would have sought to assess and manage any risk that could have occurred from a government's decision or from a social event. Since the 1970s globalisation has forced a change in the thinking of political risk and where its primary focus lies.

Globalisation is a very complex process, which can be defined in a wide variety of ways. From an economic perspective globalisation is merely the widening and speeding up of global connectedness (Lutz & Lutz, 2015:27). Yet another perspective states that globalisation has occurred because of favourable circumstances between technology, politics and economics, thus creating a society that has seen an increase in flow of foreign and domestic assets, goods, services and changes in migration. The changes in migration have created market fluidity through the immigration or emigration of workers. Market fluidity has resulted in bringing dissimilar groups into much closer proximity thus leading to the possibility of increased conflict between these groups, which can result in civil wars (Lutz & Lutz, 2015:27; Brynjar, 2005:23). Paul Wilkinson observed that modern terrorism has occurred as a reaction to globalisation (2003:124). The increased interaction and expansion of the global economy requires companies to take risks into consideration (Brink, 2004:3). The growth and

---

<sup>1</sup> The emergence during the 1970s resulted from the oil crisis. During the 1970s American oil consumption was on the rise but their domestic production was decreasing. The US became dependent on oil, which was imported from abroad. During the Yom Kippur war (which was between the State of Israel and other Arab nations) the US was one of Israel's main supporters. In response to their support of Israel, the Organisation of Arab Petroleum Exporting Countries (OAPEC) reduced their petroleum production and placed an embargo on oil shipments to the US. Ultimately this created fuel shortages and sky-high oil prices. These events created the 1970s oil crisis.

development of technology is one component that aided in the creation of globalisation. The advancements in technology have been a major factor in creating the interconnected world that exists today. These advancements in technology are of great importance to this research study as its development has changed the threat landscape in the twenty-first century and the definition of political risk.

Globalisation has been coupled with an increasingly capitalist focused economy where profit remains the main motivation. This coupling is an important factor as the capitalist focused economy informs how companies run. When you combine the interconnected world and capitalist thinking, companies can now move their operations overseas where labour may be cheaper or in the case of the oil and gas industry, they can set up operations in countries where new oil reserves have been located. The possibility of a good profit return results in companies being more willing to invest in foreign countries, of which some are unstable or unsafe, in order to achieve this goal. The oil and gas industry is no exception to this, as it yields very high profits. The extractive industry as a whole is lucrative but the most lucrative of them all remains the oil and gas extraction. As a result of this, many countries, which are rich in oil and gas, are highly dependent on the revenue they receive from this industry to drive their growth and development. This dependency makes them economically vulnerable with any disruptions having the potential of a negative impact on the particular country, as well as the global market.

Investment in oil and gas has a very long history, which can be traced all the way to British and German companies' attempt to gain access to the oil reserves located in the Middle East (Lambrechts & Blomquist, 2016:2). Explorations into oil and gas reserves during the late 1980's were predominantly conducted in areas that were classified as politically safe, which left areas of the developing world unexplored. Exploration for new oil and gas reserves is now occurring in places that are not considered politically safe and are characterized by instability and conflict. According to data gathered by Berlin, Berlin and Vrooman in 2003, sixty-five percent of oil reserves were located in the Middle East. Data collected by British Petroleum (BP) showed that in 2015 South and Central America had the highest reserve to production ratio when it came to oil production, standing at a staggering 116.96 percent, and the Middle East the nearest competitor standing at 77.11 percent (Energy Charting tool, 2016). The third region

that is oil rich is Africa. Africa is host to five oil-producing countries, which are in the top thirty oil producers in the world (Carpenter, 2015). These top five countries are Nigeria, Angola, Algeria, Egypt and Libya (Carpenter, 2015). These five countries are not the only oil producing countries in Africa; there are a number of other countries in Africa with oil reserves.

To achieve this level of financial return in the oil and gas industry, a company's investment is dependent on effective risk management and risk mitigation. This means that effective consideration needs to be taken of the potential risk factors that they could face within the industry through the utilisation of political risk analysis. Political risk analysis can be utilised by a business in order to determine whether it would be financially advantageous for them to invest or expand in specific countries. Political risk analysis will allow businesses to determine whether their investment will not receive financial returns because of the political decisions or events that occur within the country that they are potentially going to invest in.

The gas and oil industry has always been an exceptionally vulnerable sector. As was indicated by Lambrechts & Blomquist, there are a number of risk that could potentially affect the oil and gas industry such as, "corruption, taxation systems, governmental regulations, civil and labour, political instability, environmental activism, repatriation restrictions, war, external threats and terrorism" (2016:2). Despite these vulnerabilities classifying the oil and gas industry as a high-risk industry, many companies are willing to risk investing because of the potential for a high profit return. The oil and gas industry has always had a high demand placed on it by the global community. The slightest disruption of the production of oil and gas can have a severe negative impact on revenue creation for oil and gas companies. Such impacts include an increase in global political and economic tension (Blomquist & Lambrechts, 2016:2). The effects of these disruptions could become even greater as fewer oil reserves are being discovered each year and the fact that oil is a finite resource. The demand for oil, however, presents no inclination of decreasing in the near future.

As was indicated in Blomquist and Lambrechts (2016), one of the political risk factors that investors in oil and gas companies could face is the threat of terrorism. Terrorism

has always been a risk factor that the oil and gas companies have had to contend with. As such, terrorism has been classified as an industry specific risk within the oil and gas industry (Blomquist & Lambrechts, 2016:15). Since the 1990s oil and gas companies have experienced terrorist attacks. In 1997 there were an estimated 344 terrorist attacks on Algerian oil and gas companies alone (Terrorist Attacks and Threats in Algeria, 2016). The number of attacks that oil and gas companies have experienced showed a rapid increase following the 11 September 2001 terrorist attacks in the United States of America (US). This marked increase is a result of the success that terrorist attacks have on disrupting the economics of the West, in particular the US. Terrorist groups around the world have utilised attacks on oil and gas companies as their primary attack method because of the success it allows them in achieving two of their main goals: “undermining the internal stability of the regimes they are fighting, and economically weakening foreign powers with vested interests in their region” (Luft & Korin, 2003).

However, in the research conducted by Blomquist and Lambrechts, they concluded that it would never be possible to completely mitigate the threat of terrorism in the oil and gas industry (2016:15). While it may not be possible to mitigate the threat of terrorism, it is possible to manage the threat of terrorism. The threat of terrorism can be managed through the implementation of an effective political risk management strategy. This political risk management strategy should help companies be continually aware of situations on individual, national and transnational level (Blomquist & Lambrechts, 2016:15).

Terrorist attacks on oil and gas companies by terrorist groups have traditionally been conducted through the use of weapons; bombs and by infiltrating the oil and gas plantations and by holding workers hostage have traditionally been physically carried out gas companies. An example of this is the 2013 terrorist attack on the In Amena’s facility. While terrorist attacks such as these will continue to occur, there is a new rising trend in attacks on oil and gas industries: cyber-threats. In the past few years, technology has rapidly advanced. Broadband Internet was not available to everybody and Internet services providers (ISPs) restricted access to it. Now large numbers of the world’s population have access to the Internet in their homes. It has led to the advent of social media, the ability to conduct phone calls or even video chats across continents.

Technological products, such as phones and computers, are continually changing and improving to be better than products that are already on sale. Apple has brought out new models of the iPhone once every year for the last eleven years, each model seeking to be better than the previous and more user-friendly than any other phone on the market. These advancements have led to industries becoming increasingly digitalised. As a result of this increased digitalisation companies are placing themselves at a greater risk of being infiltrated and hacked by external sources. The oil and gas industry is no exception to the risk of cyber-threats.

According to Alexander Polyakov, the founder of ERPscan a security firm that specialises in software security, the oil and gas industry is one of the industries that is most plagued by cyber-attacks (Keane, 2015). Cyber-threats against the oil and gas companies can be classified as a more recent phenomenon, with attacks only starting and being documented in the last ten years (Polyakov, 2016). One of the most well-known cyber-attacks against the oil and gas industry, according to Keane, occurred in 2012 when Saudi Aramco, Saudi Arabia's state-run oil giant was hacked (Keane, 2015).<sup>2</sup> During this attack Saudi Aramco computers were wiped clean by a virus and replaced by an image of a burning American Flag (Polyakov, 2016). The Cutting Sword of Justice claimed responsibility for this attack. The group stated that they aimed to stop oil production and its flow into the international market because of the Al-Saud regime utilising Muslim oil resources.

Cyber-attacks can be carried out from a great distance but will still have the potential to put the safety of oil and gas companies' workers at risk. Depending on the method of attack, cyberterrorism attacks can result in deaths and injuries much like physical attacks would. Death and injury, as a result of cyber-attacks, can occur if hackers violate safety measures, change alarm settings and disable communications between workers on the field (Keane, 2015; Polyakov, 2017). Cyber-attacks can be coordinated with physical terrorist attacks that will allow for greater damage and casualties. The fact that cyber-attacks can be conducted from a distance makes it is possible for attacks to occur in regions that are not characterised by political upheaval, instability and conflict.

---

<sup>2</sup> The attack on Saudi Aramco will be further examined in Chapter Four of this research study.



According to data gathered by ABI Research it is predicted that by 2018 oil and gas companies will be spending roughly US\$1.87 billion on cyber-security alone (Polyakov, 2017). Despite this predicted increased expenditure on cyber-security the oil and gas industry still fall victim to cyber-attacks because of a lack of awareness and lack of trust between oil companies (Polyakov, 2017). In Africa there are countries that refuse to acknowledge the threat of cyber-attacks, despite being the third oil rich region in the world. (Shaw, 2018). Ultimately there is a struggle in African countries to build technical and financial capacity that is needed to target, monitor and stop such attacks (Shaw, 2018). The refusal to acknowledge this threat and not having the capabilities to prevent cyber-attacks is not just an issue in African countries, it is a problem for most countries and industries. There has been no identifications of risk indicators or how the threat can be managed and there is a lack of transparency in sharing methods to prevent cyber-attacks in the oil and gas industry. Additionally, the oil and gas industry still has not fully acknowledged the threat that cyber-attacks pose to their daily operations or how it will increase the political risk they already face.

## **1.2 Preliminary Literature Review**

This study will be divided into four broad fields of literature, which will focus on the concepts necessary for this research study. The first field of literature will provide a theoretical grounding that is needed in this study. This will be conducted by looking at the literature relating to political-risk analysis. In looking at this first field of literature, the following theories that are related to political risk will be examined rational choice, problem-solving and decision-making theories. Political risk is becoming increasingly more important in this interconnected global society. Despite the importance of political risk being recognised, it remains a complex subject. There is a great deal of literature that covers the topic of political risk and it has been covered by plenty of influential scholars. Two of these influential authors are Simon and Kobrin who both have a number of works that address political risk, such as Simon's 1982 article *Political Risk Assessment: Past Trends and Future Prospects* and Korbin's 1979 article *Political Risk: A Review and Reconsideration*. Work, which has been published by the following influential authors, will also be examined to further develop the theoretical grounding: Robock (1971), *Political Risk: Identification and Assessment*, Fitzpatrick (1983), *The Definition and Assessment of Political Risk in International Business: A Review of the*

*Literature*, Alon and Martin (1998), *A Normative Model of Macro Political Assessment* and Alon, Gurumoorthy, Mitchell & Steen (2006), *Managing Mircopolitical Risk: A Cross-Sector Examination*.

The second field will focus on industry specific-risk in the oil and gas industry. The purpose of the section will be to use literature to establish that a connection exists between the gas and oil industry and political risk. One of the articles that will be used predominantly in order to achieve this is *Managing Political Risk in the Oil and Gas industry* published by Berlin, Berlin and Vrooman in 2003. While their article will be used predominantly in this section, it will not be the only source of information utilised in looking at industry specific risk in the oil and gas industry. Lax (1983), *Political risk in the International Oil and Gas industry*, Frynas and Mellahi (2003), *Political risks as Firm Specific (Dis)advantages: Evidence on Transnational oil Firms in Nigeria* and Alon *et al.* (2006), *Managing Micro political Risk: A Cross-Sector Examination*.

The third field of literature will focus on cyber-threats. Cyber-threats are a relatively new subcategory of terrorism. Thus, in order to gain a better understanding of cyber-threats additional literature will be utilised in order to better understand this new form of terrorism and establish what threat it poses. This literature will aim to show that there are different types of cyber-attacks that utilise different methods, have different targets and have different motivations. Examples of the literature that will be reviewed are as follows: Lachow (2009), *Cyber Terrorism: Menace or Myth*, Shattuck, Slaughter and Mittal (2017), *Refining at risk: Securing downstream assets from cyber-security threats*, Ernst and Young (2014), *Oil and gas cybersecurity: Penetration testing techniques*, Weimann (2004), *Cyberterrorism: How Real Is the Threat*, Polyakov (2017), *Cyber Security Risks To Be Aware of In The Oil and Gas Industries*.

The fourth and final field will look at the influence of cyber-attacks on the oil and gas industry. As this is considered to be a relatively new field of study, there is only a limited amount of literature that focuses on cyber-attacks as an industry specific threat to oil and gas companies. The literature that will be looked at will be reports published by the firm Ernst and Young titled *Oil and gas cybersecurity: Penetration testing techniques*. Additionally, another reports such as the European Union Agency for

Network and Information Security' (ENISA) report (2017) on *Cyber Security Information Sharing in the Energy Sector*. To further develop the understanding of the influence that cyber-attacks have on the oil and gas industry two selected cases of oil and gas companies, which have experienced cyber-attacks will be examined and compared. This section will look at each case individually and look at how the attack influenced oil and gas companies that were targeted in the attack.

The first is the 2012 attack on Saudi Arabian Oil Company, more commonly known as Saudi Aramco which, is a Saudi Arabian national petroleum and natural gas company. The article written by Perlroth (2012) and Pagliery (2016) and the writings of Bronk (2016), as well as other sources will be used, to outline how the attack was carried out and its impact on Saudi Aramco. The second cyber-attack occurred in 2014 and involved dozens of oil and gas companies in Norway, including Statoil, one of Europe's biggest suppliers of energy.<sup>3</sup> Information on the events of the attack on the Norwegian companies will be gathered from an article documenting the attack written by John Leyden (2014) as well as other sources. Statoil will be the focus of the impact of the attack that occurred in Norway. Following the 2013 In Amenas terrorist attack, in Libya, Statoil undertook an assessment to look at the risk of an attack occurring again (Boman, 2015). After the assessment's completion, Statoil determined that cyber-security attacks would act as a long-term threat to their operations and not physical attacks.

### **1.3 Research Problem and Research Question**

Political risk analysis continues to be an increasingly important field in today's world, which is continually becoming more interconnected through globalisation and technological advances. Furthermore, the increased levels of foreign investment have added to the importance of political risk analysis. The oil and gas industry is an extremely lucrative business, which has led to numerous international companies seeking to invest in the industry. The majority of oil and gas reserves are located in

---

<sup>3</sup> It is important to note that this research study is aware that in 2018 the company changed their name to Equinor. However, for the purpose of this research the company's former name Statoil will continue to be used.

areas that are typically characterized by political upheaval, instability and conflict. Most oil and gas reserves are located in these troubled areas, with increased political risk, which result in investments into reserves located in these areas being a high-risk investments. Despite the high risk associated with these investments, firms are often willing to accept the risk because globally the business environment is harsh and there is the potential of high rewards in this industry. The high risk, which is associated with the oil and gas industry, is further highlighted by the increased number of terrorist attacks.

Terrorist attacks are one of the primary political risk factors which oil and gas companies face. Since 1986 attacks on refineries have been documented as only happening infrequently (Lia & Kjøk, 2004:109). During the period 1992 to 1998 according to The International Terrorism: Attributes of Terrorist Events (ITERATE) there were 5000 attacks. However, only 22 of these attacks were documented as being directed at oil and gas facilities. Terrorist attacks against the oil and gas facilities only increased following the September 11 terrorist attacks, as oil and gas companies become the focus of terrorist organisations (Yetiv, 2011:109). Terrorist organisations utilise attacks on oil and gas companies in order to destabilise the economies of the West and in particular the USA. Evidence of the increase is seen in Iraq, which is one of the main suppliers of oil to the USA, where between 2003 and 2006 there were an estimated 374 attacks on oil pipelines during that three-year period. Even though terrorist attacks are a known risk in the oil and gas industry, the necessary security measures to mitigate or manage the threat of attacks are not always put in place by the different oil and gas companies.

Political risk analysis has become necessary in order to ensure the safety and security of the personnel working at the plantations with the increased level of risk of terrorist attacks that oil and gas companies now face. It has resulted in a change in the way in which the oil and gas industry thinks about risk. The change in thinking in risk is necessary to help put in place the needed security measures that will limit the damage that can be done to the infrastructure of oil and gas plantations; damage to plantations that would cost companies millions to repair. There is however a new threat to oil and gas facilities, that will force a change in how oil and gas companies think about risk

again. The new threat facing oil and gas facilities is cyber-threats, which is a new sub-field of terrorism.

Cyber-threats indicate that the methods of terrorist attacks are changing in nature in order to mimic the rapid development of technology. Traditionally most terrorist attacks are characterised as being conducted in countries or regions that have political upheaval, instability and conflict. However, terrorist attacks are not solely carried out in regions or countries that are politically unstable. The 11 September attack in the United States of America, conducted by the terrorist group al Qaeda, is the best evidence of such attacks. The attack consisted of four USA airlines being hijacked, two crashed into the north and south towers of the World Trade Centre complex. The third crashed into the Pentagon. The fourth crash-landed in a field, after passengers overwhelmed the hijacker. This is not the only example of terrorist attacks being carried out in countries that are viewed as politically safe. There are a number of different incidents such as this one. Following the 11 September attack, the leader of al Qaeda, Osama Bin Laden, published a statement where he announced that the best method of achieving their primary goal of crippling Western economies was by attacking oil and gas companies (Luft & Korin, 2003). Since Bin Laden published this statement numerous attacks have been carried out against the oil and gas facilities around the world. Following the US invasion of Iraq, Iraqi pipelines were repeatedly targeted which cost them more than US\$ 10 billion in oil revenues, Mexican pipelines were targeted six times in 2007 the People's Revolutionary Army (ERP), which resulted in several supply shortages and temporary closure of several of their factories as well as the In Amenas attack which will be discussed further in the next section.

As stated in the background to this study, explorations into oil and gas reserves are now being conducted in places that have political upheaval, instability and conflict. Attacks on oil and gas reserves in regions classified as such have occurred. An example of such attacks can be seen in the 2013 attack on the In Amenas. The In Amenas was a severe attack, which was carried out against a gas installation and resulted in one of the most serious international crises Statoil has ever faced. However, cyberterrorism on oil and gas facilities is not limited to areas categorised by political instability and conflict. Cyber-attacks can occur in regions where there is political stability. The previously

mentioned attack that occurred in Norway in 2014 is an example of just such a cyber-attack. The extent of the influence that the attack in Norway had on the various oil facilities remains unknown, as there is only a limited amount of information available that covers the event (Bryne, 2014). More importantly the number of cyber-attacks has increased annually, which poses the question of how the oil and gas industry is affected by these attacks and if the industry is equipped and has the capabilities to deal with the new threat that faces them. Consequently, the main research question of this thesis will be:

- Do cyber-threats increase the political risk which oil and gas companies face?

In order to help supplement and support the main research question sub-questions have been developed:

- Which vulnerabilities of cyber-threats can be identified and used by companies in the oil and gas industry in order to help them manage and/or mitigate these risks?
- Will cyber-attacks result in oil and gas companies losing revenue and halt their daily operations?
- Can international oil and gas companies mitigate the risk of cyber-threats, or is this risk something that can only be managed?

#### **1.4 Objective and Relevance of the Research Study**

As pointed out previously, following the 11 September attacks, terrorist attacks carried out against the oil and gas industry started to occur far more frequently. The reason for this is Bin Laden's statement, which identified the oil and gas industry as the most attractive option of attack to achieve their primary goal, of destabilising Western economies. The number of terrorist attacks have continued to increase through the years. Coupled with the increase of attacks is the fact that there have been fewer discoveries of new oil and gas reserves. In addition, there are numerous oil and gas companies already in existence this is something that will continue to increase rapidly. As a result of these two factors companies have a greater willingness to accept the high risks. The high risk placed on the oil and gas industry could only increase now as a result of the growing trend of cyber-attacks facing the industry. As cyber-threats are a

recent phenomenon, there has been little to no research undertaken which seeks to identify vulnerabilities to cyber-attacks in the oil and gas industry. The primary purpose of this research is to identify the influence that cyber-threats have on political risk for the oil and gas industry. Along with discovering which vulnerabilities to cyber-threats can be identified by companies in the oil and gas industry and can be used to help them manage and mitigate the threat of cyber-attacks.

### **1.5 Research Design and Research Methodology**

The main purpose of this research study is gauging the influence that cyber-threats have on the oil and gas industry. Additionally, vulnerabilities to cyber-threats will be identified. As well as evaluating how oil and gas companies can utilise these identified vulnerabilities to mitigate and manage the political risk of cyber-threats. The methodology used in this research study will be primarily qualitative. Qualitative data provides in-depth knowledge (Burnham, Lutz, Grant & Layton-Henry, 2008:40). In-depth knowledge comes as a result of the vast amount of data that qualitative data generates from the findings in specific cases. However, a limitation to the findings acquired through qualitative data, is that they cannot be used to make generalisations as they are focused on specific cases. The direction of theorising that this research study utilises is an inductive direction. Inductive research is an observation of the empirical world that results in “a general topic and vague ideas” that will be established and later refined and elaborated into more precise theoretical concepts and propositions (Neuman, 2014:70).

The research design of this study will be a comparative design. Burnham *et al.* state the comparative design within political science is one of the most important methods of research (2008:66). Comparative design allows for the discovery of a common cause between the cases. This allows for generalisations to be formed (Burnham *et al.*, 2008:66). When it comes to making these generalisations, it is very important to be careful, as they do not always hold the truth. Normally in a comparative design, only a small number of cases are selected and utilised. A limitation with comparative design is that it is often difficult to find comparable cases. To help in selecting comparative cases it is necessary to decide between the two basic designs of comparative research: the most similar and the most different research design (Burnham, *et al.*, 2008:73). For

this study cases have been selected utilising the most similar research design. With a most similar design the independent variable (x) in all cases is the same but they differ in the dependent variable (y) and all other variables. For this study the independent variable is cyber-attacks on oil and gas facilities. The dependent variable is risk indicators of cyber-attacks that can be identified by the oil and gas industry. These risk indicators will differ as a result of different circumstances found in the attacks such as: different facilities, difference in the code written for the cyber-attack and there could be a difference in the sophistication of the attacks. Ultimately, there is a possibility that the risk indicators identified could vary between the two different cases and not have any similar risk indicators.

Two cases have been selected for the comparative design of this study. The cases, that will be used, are the following: the 2012 cyber-attack on Saudi Aramco and the 2014 cyber-attack on Norwegian oil companies, including Statoil. These two cases have been selected, as they are the most documented cyber-attacks on the oil and gas facilities. Looking at these attacks will be interesting as they will establish whether or not cyber-attacks increase the risk faced by oil and gas companies as well as establish whether cyber-attacks can be either managed or mitigated by oil and gas companies. Of particular interest is Statoil's response to the Norwegian attack, as following the 2013 In Amenas attack, they conducted a full risk assessment in which they determined that their greatest threat in the future would be cyber-attacks.

This study will predominantly utilise secondary sources in its research. The reason for this is that research on political risk faces certain limitations. One particular limitation is the fact that most risk analysis bureaus as well as oil and gas companies prefer not to publish their security management models to the wider public. These models are often classified as intellectual property. In addition to this there is no funding involved in this research study therefore the use of secondary sources is useful as it is a more cost-effective method (Burnham, *et al.*, 2008:43). The greater part of this study will be based on secondary information and data that is gathered from academic books, journals, and reports, which can be found at both the Stellenbosch University library and their online database, along with additional information found online. In order to ensure the information found in these sources is reliable they will be compared to ensure the



information gathered is accurate. The additional information acquired from online sources comes from trusted domains and trusted authors.

Additionally, this study will be predominantly descriptive in nature. Descriptive research, according to Neuman, begins with a “well-defined issue or question and tries to describe it accurately” (Neuman, 2014:39-40). At the end of this research study, a detailed explanation of the problem should be given, which provides a sufficient answer to the initial research question (Neuman, 2014:39). This research study will be descriptive in nature when it comes to trying to explain the way recent cyber-attacks have had an influence on the oil and gas industry. Moreover, a descriptive approach seeks to answer the questions of ‘how’ and ‘who’ (Neuman, 2014:39). The main question of this research is how cyber-attacks increase the risk faced by the oil and gas industry. According to Neuman, it can be hard to separate descriptive and exploratory research, which can lead to these two forms of research being blurred, which is the case with this research study (2014:38). This research study will be exploratory due to the fact that it is seeking to provide a new insight into and perspective to the topic. The focus on cyber-threats is a rather new phenomenon. When looking at political risk within the oil and gas industry, there has been very little research on this topic. Explanatory research seeks to answer the question of ‘why’. Answering the question of ‘why’ builds on descriptive research and helps in trying to explain why something occurs (Neuman, 2011:40). The focus of this thesis is entirely on the oil and gas industry resulting in research being on a micro-level.

### **1.6 Limitation of Research Study**

In this research study the focus is on the political risk of cyber-threats and how it influences the oil and gas industry. One of the limitations to this study is the fact that cyber-attacks and cyber-security within the oil and gas industry is a topic that is now only starting to attract the interest of academic scholars. As a result, there is a limited amount of literature available on this topic. In order to overcome this limitation, documented attacks against oil and gas companies will be looked at to help identify risk indicators. In addition, the extent of political-risk analyses being used within companies will be examined by looking at their practices to see if oil and gas companies take into account cyber-threats.

A second limitation of this study is that limited primary data will be utilised in this research study due to the lack of information sharing surrounding cyber-attack and cyber-security in the oil and gas industry. A further limitation of this study is that interviewing a terrorist would present a number of dangers to the author. Conducting interviews with hackers would be difficult as most hackers operate anonymously, making it difficult to identify individuals for this study to potentially interview in order to collect primary data. Overall, these limitations will be overcome by using the relevant data from sources that are found online, in newspaper articles and in journals on cyber-threats in the oil and gas industry.

As previously stated, a further limitation of this study relates to the fact that it is difficult to gain access to different risk management companies' models on risk, as these models are often regarded as the intellectual property of these companies. As a result, this limits this studies' ability to see how oil and gas companies have already addressed the security threat posed by cyber-attacks. Through the use of other sources on the topic, such as reports published by Deloitte and Ernst and Young along with new articles, it will be possible to overcome this limitation and gain a picture of how oil and gas companies have been addressing the issue of cyber-attacks.

### **1.7 Outline of the Research Study**

Chapter Two of this research study will utilise secondary data. The data will be utilised to provide a greater understanding of the theoretical grounding needed for this research study. The theory of political risk is founded in problem-solving, rational choice and decision-making theory. It would therefore be prudent to begin with the conceptualisation of these theories. Following the conceptualisation of these theories, this study will provide a report on the concepts of risk, political risk, and macro- and micro-risk. Within this section industry-specific or firm-specific risk will be explored closely. In Chapter Two a conceptualisation of risk management and mitigation will be provided. Chapter Two will conclude with the provision of the conceptualisation of 'cyber-threats' and 'cyber-attacks'.

In Chapter Three secondary data will be used to further contextualise the research study. This Chapter will provide an account of the development and evolution of cyber-threats and cyber-attacks on the oil and gas industry, as well as identify vulnerabilities to cyber-threats. In looking at the development of cyber-attacks in the oil and gas industry, the focus will be on the ways in which the different sectors' operations are vulnerable. After establishing how cyber-threats can be carried out on different operations in the oil and gas industry the vulnerabilities which put oil and gas companies at risk of being attacked will be further examined.

Chapter Four will utilise the data that has been presented in Chapters Two and Three to critically analyse it through the theoretical framework created in Chapter Two. The vulnerabilities to cyber-threats against oil and gas companies, identified in Chapter 3, will be used to analyse the two cases. Both the cases of cyber-attacks against Statoil and Saudi Aramco, will be analysed to establish which vulnerabilities to cyber-threats should have been utilised to identify and forewarn the companies about the cyber-attacks. In looking at these attacks, their influence will be examined in order to assess if they increased political risk for companies in oil and gas. Lastly, the possibilities of how oil and gas companies can effectively mitigate the risk of cyber-attacks will be examined or whether it is something that can only be managed.

Chapter Five will provide the conclusion of this research study. This will be conducted through utilising the research that was done in Chapters Two, Three and Four and will be framed by the research question of this study. The results of the analysis from Chapter Four will be critically evaluated. Through this critical examination suggestions for possible improvements will be reflected on. Chapter Five will ultimately conclude with the provision of suggestions of what can be explored in future research within the field of political risk analysis in the oil and gas industry.

## **1.8 Conclusion**

This chapter has provided a general introduction to the research problem. Along with this an outline has been given of the objectives and relevance of this research. The research design and methodology of this thesis has been outlined and explained. Lastly an outline for the remaining chapters of this research study has been provided. The

research problem of this study necessitates examination and analysis of vulnerabilities to cyber-threats, which can be identified to help manage and mitigate this threat to the oil and gas industry. The cyber-attacks carried out on Saudi Arabia's facility Saudi Aramco in 2012 and the attack on Statoil's facility based in Norway in 2014 will be used as the case studies for the most similar comparative design of the study. Three sub-questions have been developed in order to supplement and support the main research question. These questions will seek to examine whether cyber-threats will result in an increase in political risk and how it will influence the production and revenue of oil and gas companies. The last sub-question of this study explores whether or not it is possible for oil and gas companies to mitigate the risk of cyber-attacks or if the only real option that oil and gas companies have is to manage the risk of cyber-attacks.

## Chapter Two: Theoretical Perspective and Contextualisation

### 2.1 Introduction

The management and mitigation of risk is forecasting, and is set to become increasingly more important to international companies. One of the factors, which has resulted in the increased significance being placed on forecasting, is globalisation. Globalisation has led to closer economic cooperation in the global system and greater mobility of capital. The global environment is rapidly becoming far more complex with the aid of technological developments. Political and social changes in the world are also occurring at a much faster pace than in the past. This increased pace is the result of the rapid growth of technology and has led to increased risks to global stability. As stated in Bremmer and Keat (2009), this is why more value will be placed on being able to successfully manage political risks that companies could potentially face. Within the oil and gas industry, this is especially true as risk management and mitigation has always been of great significance within the industry.

The importance of risk management and mitigation is the result of the fact that investments within the oil and gas industry have the ability to exceed billions of US Dollars. In order to achieve such high returns, management and mitigation of risk is of a great necessity. Terrorism has been a long-standing threat that the oil and gas industry has faced but now the nature of the terrorist attacks is changing to mimic the rapid development of technology. Thus, non-state actors such as corporations, religious groups, violent non-state actors, such as terrorist organisations, can move to cyber-attacks on the oil and gas companies. As such, it is necessary for oil and gas companies to develop techniques to manage and mitigate the risk that cyber-threats pose to the oil and gas companies. In order for oil and gas companies to properly manage and mitigate the risk that cyber-threats pose, it is necessary to identify the risk indicators of a cyber-attack occurring.

The purpose of this chapter is to provide the theoretical foundation, on which this research study is based. The first section will examine rational choice theory, problem solving and decision-making theory. The second section will explain the main concepts and provide conceptualisation of them. The conceptualisation of these key concepts

such as risk, political risk and cyber-threats is essential to this research study as it provides the in-depth knowledge which will be needed for analysis later.

## **2.2 Rational Choice Theory, Problem-Solving and Decision-Making Theory: A Theoretical Grounding**

This section will make use of older sources of literature as new literature has continued to be heavily dependent on the older sources of writing on rational choice, problem-solving and decision-making theory. Rational choice theory emerged from traditional economic theory. Rational choice theory has historically been a dominant paradigm of thinking within economics, as well as other academic disciplines, such as political science. Traditional economic theory introduces the idea of a man who is economical as well a rational thinker (Simon, 1955:99). Traditional economic theory referred to this man as the rational man.

The rational man, according to economic theory, is assumed to have the relevant knowledge of the important aspects of the environment in which he works. However, it is important to be aware that this knowledge of the environment may not be complete, but it will be enough to enable him to make the correct decisions. The rational man is considered to be capable of choosing the best course of action. Traditional economic theory provides the foundation on which to build a theory. Rational choice theory can be utilised to help understand human behaviour. Traditional economic theory focuses on the individual rational man while rational choice theory focuses on the behaviour of the decision-making unit (Green, 2002:4). For the instance of this research study that unit refers to international oil and gas companies.

In international or national oil and gas companies, managers or executives continually make decisions on current or future plans for the company or will select the best solution to a problem that may have arisen. Making such decisions is essentially a core element of the daily work of any business manager (Simon, Dantzig, Hogarth, Plott, Schelling, Shepsle, Tversky & Winter, 1987:11). For managers of oil and gas companies, these decisions can cover a wide range of issues ranging from strikes of oil rig workers; changes or the introduction of new petroleum laws, which could potentially affect a company's interests; and questions regarding security against

threats and acts of terrorism. Managers are required to make the choice of which problems need to be addressed and especially which one needs to be dealt with first. In order to do this, decision-makers will utilise the knowledge of the environment that they have to help aid them in selecting the best alternative and deciding what needs to be done in order to continue to achieve the company's primary goals. An example of this can be seen in decisions regarding whether to expand operations into new regions or whether production should be increased which can make the company more profitable. When managers decide which issues need attention, set goals and come up with a plan of action, these three actions are referred to as problem-solving (Simon *et al.*, 1987:11). When managers evaluate and select the best alternative actions, this process is referred to as decision-making (Simon *at al.* 1987:11).

One of the first steps that a business should take in decision-making, when it is seeking to potentially expand its business into a new country, is to conduct a political risk analysis. The focus of political risk analysis is placed on optimizing the profit of the investment. Political risk assessment is generally understood to help with decision-making problems. A political risk assessment for a company will focus on whether or not they should go forward with investing in a new region (Brink, 2004:30). However, a critique put forward is that these models are only normative models of what an idealised decision maker would do (Tversky & Kahneman, 1986:251). As a result, these models do not necessarily take into account the decision-making behaviour of a normal individual's daily decision-making process (Tversky & Kahneman, 1986:251). Despite the fact that the focus is on an idealised decision-maker, these models remain useful as they provide knowledge about and insight into why certain decisions in a company are made. The argument, which supports the continued usefulness of these models, is that individual decision-makers are considered to be more effective in the pursuit of their own goals.

It is believed that individuals who are both rational and organised tend to have a better chance of achieving their goals, especially in a competitive environment. This is particularly true when there are incentives and opportunities that allow for individuals to learn from their experiences (Tversky & Kahneman, 1986:251). Thus, it makes sense to perceive choice as a process of maximisation. This logic applies to the oil and gas

industry as well. An oil and gas company will have an already well-established set of preferences and an ability to effectively determine their best alternative action (Simon, 1955:99). Examples of this in oil and gas companies can be found by looking at investing in new oil fields, whether to acquire new equipment or if they should expand operations to a new country. This requires individuals and organisations to act rationally in a competitive environment. In a competitive environment, the best decisions result in an increased profit for oil and gas companies (Tversky & Kahneman, 1986:251). Allowing oil and gas companies to achieve their primary business goal of making a profit.

An additional factor that the rational actor has to focus on in the decision-making process is reducing or minimising uncertainty. The rational actor will seek to reduce this uncertainty by applying expert knowledge and experience to the topic (Simon, 1955:99). Knowledge and experience may not always be sufficient. When this happens and a decision-maker cannot identify a suitable method of minimising the risk that they could face, they are more likely to withhold their investment or remove their investment from a region (Brink, 2004:30). In the oil and gas industry investors could choose to abstain from investing in a new country or consider pulling out. One of the ways for decision-makers to avoid this uncertainty is to ensure that they follow the basic steps of decision-making. According to Chicken, decision-making requires the conceptualisation of the plan on investing in new projects or expanding operations, which already exist (1986:40). This is done through utilising internal or external actors in conducting studies in order to determine the possible outcomes and to plan how to implement the decisions that have to be taken (Chicken, 1986:40).

In later literature, Simon *et al.* (1987) provides an alternative six steps to follow in order to reduce uncertainty:

1. Identify what the problem and/or opportunities are and determine which to deal with first
2. Set goals to help collect the necessary information
3. Develop as many suitable alternative plans as possible
4. Evaluate the various alternatives
5. Select the best alternative



6. Implement the alternative selected and re-evaluate the alternative in order to ensure that it has been effective  
(Simon *et al.*, 1987:11).

Decision-makers are required to take into consideration different alternatives, calculate the consequences of applying the different alternatives, reduce the uncertainties that might accompany the best alternative and ultimately find a solution that will satisfy investors (Simon, 1979:11). In the instance of political risk analysis, it provides information to decision-makers, which highlights the different political risks, that could possibly affect the profitability of projects for a specific company. Once the company has the political risk analysis, they can develop strategies on a method to manage the identified risks (Brink, 2004:30). In the case of this research study oil and gas companies would obtain information identifying vulnerabilities that put the oil and gas industry at risk of being a target of a cyber-attack.

### **2.3 Risk**

It was during the 1970s and 1980s that the concept of risk began to emerge and became of greater concern to different industries and all levels of government began to discuss it. Risk is still being discussed at a governmental level, but it is now also being discussed at a business level. With increased importance placed on the concept of risk, numerous types of risk started to emerge. Some of the predominant types were business risk, investment risk and political risk (Kaplan & Garrick, 1981:11). The main focus of this study is on political risk. One of the issues that arose from the study of risk, is that there are numerous definitions, developed over the years seeking to explain it. Most of these definitions of risk tend to be quite broad. An example of a broad definition of risk is found in Bremmer and Keat's writing in which risk is defined as "the probability that any event will turn into measurable losses" (2009:4). Another common definition that is used in defining risk states that: it is when there has been change, damage or loss that had not been present previously (Lax, 1983:8). Lax added to the conceptualisation of the definition of risk stating that it is dynamic and often deals with change and that "current conditions are not risks; rather, risk stems from changes in those conditions" (Lax, 1983:8). The definition is conceptualised further by Vertzberger who states that risk is defined as "the likelihood that validly predictable direct and indirect consequences with potential adverse values will materialise, arising from particular events, self-behaviour, environmental constraints, or the reaction of a third party"

(1998:22). Vertzberger identifies that risk can be the result of both direct and indirect actions. Thus actions, which are not directed at a specific company or industry, can still impact negatively on these companies.

Examples of common words associated with risk are: threat, loss, danger, vulnerability, hazard and misfortune. These words support the uncertainty that comes with risk because of the potential negative or positive outcomes that could occur. Hough defines risk as “uncertainty that is associated with a particular event and the potential consequences of these events” (2008:1). Hough’s definition helps show how risk and uncertainty, as well as instability, are often used interchangeably. However, uncertainty and instability are merely properties associated with risk. Brink explains this through the following statement, “risk is a more objective measurement of the amount of doubt, in contrast to the more subjective nature of instability and uncertainty” (Brink, 2004:19). Uncertainty implies that there is an “inability to determine the probability or the impact (or both) of a certain future event” (Bremmer & Keat, 2009:16). Ultimately, this creates the understanding that risk should be used when looking at a situation where there is uncertainty and the outcome is unknown and could have potential negative outcomes (Hough, 2008:4-5). Hough, thus provides one of the most well-rounded definitions of risk.

Kaplan and Garrick add to this definition by stating that there will be some form of damage or loss to an investor’s property (1981:12). They portray their definition of risk through the use of a basic equation which appears as follows: Risk = Uncertainty + Damage (Kaplan & Garrick, 1981:12). Ultimately, both risk and uncertainty deal with what could potentially happen in the future but as has been stated risk is capable of calculating probabilities. Thus, it is possible for risk to have the opportunity to protect your company and create a plan for anything that could happen in the future. Uncertainty, on the other hand, is incapable of providing such opportunities. Even if uncertainty exists, a company can decide to take the risk, as there is the potential for a positive outcome. There is also possibility for a company to exploit these uncertainties (Brink, 2004:21). More often than not smaller companies are more willing to take such risks. Companies are willing to accept this high risk because of the potential high return, in the form of profit (Bray, 2003:299). This is particularly true for the oil and gas

companies. An example is when oil and gas companies will occasionally invest in new oil fields despite the high risks, as there are a limited number of new oil reserves being discovered, because of the potential high profit return.

## **2.4 Political Risk**

The first issue that has to be acknowledged about the concept of political risk is the continued lack of consensus on how political risk is defined. Even in early writing on political risk, this issue is identified by Fitzpatrick who states that the definition of political risk can range between general definitions and specific definitions (Fitzpatrick, 1983:249). However, the concept of political risk is becoming increasingly more important. The greater importance of political risk stems from the tectonic shifts, which have occurred in geopolitics in the last three decades as they have drastically altered the international landscape (Rice & Zegart, 2018). This shift in geopolitics stems from the process of globalisation and the end of the Cold War. These two factors resulted in the distance between markets and politics shrinking, as well as the distance between producers and consumers. The shrinking of these distance has created an interconnected world and global economy that has forced companies to take risk into greater consideration (Brink, 2004:3). This interconnected world has made it necessary for companies to be able to forecast if there is any potential risk and have a strategy in place in order to address such a risk should it arise. However, the greatest effect these changes have had is that they have forced a change in the thinking of political risk and where its focus lies.

For a long time, political risk was predominantly associated with its application to an investing company and the host government of a country. One of the earliest definitions of political risk has the focus of the definition being placed on the whole environment instead of being placed on isolated events. Robock (1971) in his writing argues that political risk in a business happens when there are disruptions that are caused by political change. However, it is very difficult to anticipate when something such as this will occur. A company's main focus is ensuring that they make a profit and achieve any other goals that they may have set, as was outlined in the section in the grounding theory section of this chapter. If these outcomes are affected by political changes then it is perceived as a risk. Robock states that there are three potential manners in which

political risk can exist in the business environment which supports his definition: “(1) when discontinuities occur in the business environment; (2) when these are difficult to anticipate; and (3) when they result from political change” (1971:7).

Within Robock’s definition of political risk he stated that government interference in business affairs is the primary reason that investors do not make a return on their investments, thus government interference is the primary source of political risk. One of the definition’s that best supports Robock’s writing is found in Kobrin (1979). Kobrin, in developing his definition of political risk, cites the definition of political risk developed by Weston and Sorge’s, which states that “political risk arises from the actions of national governments which interfere with or prevent business transactions, or change the terms of agreements, or cause the confiscation of wholly and partially foreign-owned business property” (Kobrin, 1979:67). A critique of this definition is that only select groups or majority groups and foreign business operations and investment are negatively impacted by a government’s policies or society’s actions (Simon, 1982:68). Despite this critique, Weston and Sorge are not the only authors on political risk that support this definition. Fitzpatrick (1983) continued the support for Robock’s writing as he defined political risk through a host government and a foreign business company’s relationship (1983:249). This understanding of political risk has remained within the definition of political risk as later writing further simplified Robock’s writing by stating that it is ultimately viewed as originating from two main sources: nationalisation and expropriation (Alon, Gurumoorthy, Mitchell & Steen, 2006:624). Despite the strength of Robock’s definition it would not go unchallenged.

While Robock’s definition of political risk may have continued to be supported in later literature, other authors have challenged the validity of Robock’s (1971) definition. More recent authors make the argument that there is far too much importance placed on the factor of political instability and government actors. Firstly, Kobrin and a few years later Lax, argued that the events, which are usually associated with political instability, only happen infrequently (Kobrin, 1981; Lax, 1983). Kobrin (1981) states a consequence of the focus being predominately placed on the more drastic events of political instability such as coups or revolutions has caused a lack of attention to be paid to events that were categorised as being less drastic or ‘eye-catching’ (Kobrin,

1981:253). This critique is further expanded, by Kobrin (1981), who stated that these lesser events can actually be just as damaging. Kobrin states that these smaller events happen far more frequently than the more drastic events and thus these events are very under-analysed (Kobrin, 1981:253). It is in Kobrin's (1981) article that the best examples of how lesser events are not considered nearly as much as major events. Kobrin conducted a survey asking managers of international companies to list their top twelve contingency plans. The majority of these companies ranked civil disorder first and external war as second, nothing else came anywhere close to these (Kobrin, 1981:252). More literature on political risk written by Jakobsen (2012) agrees and supports the critiques on Robock's definition, put forward by Kobrin, even though it was published thirty-one years later. Jakobsen supported the fact that lesser events can be just as damaging and they remain under-analysed (Jakobsen, 2012:30).

Ever since the 1990s the majority of political risk scholars such as Butler and Joaquin (1998), Wells (1998) and later Jakobsen (2012), have come to recognise that government intervention along with policies are actually the most common forms of political risk. Focus in recent times has turned to low-key changes made by government as they now pose the greatest threat to international companies. Thus, as previously mentioned attention was now being paid to the less dramatic events, which both Kobrin (1981) and Jakobsen (2012) had identified as being under-analysed. These low-key changes are more threatening than the impact of the actions of non-governmental organisations, such as terrorism, kidnapping and sabotage. Even though from this perspective terrorism is determined to not affect companies as much as low-key government changes, its effects can still be severe. The damages and effects of these attacks can end up costing companies millions of dollars in damage and in very severe cases the death of employees.

While earlier definitions, such as Korbin's, were key to the development of political risk, much criticism was placed on these definitions. A few years later Fitzpatrick (1983) put forward a critique against these definitions, arguing that the early definitions of political risk were far too narrow. This particular critique was supported and further expanded fifteen years later by Alon and Martin (1998). Alon and Martin (1998) identified the same critique as Fitzpatrick, but furthered their critique through the

identification of two other key problems from these early definitions. As a result of these narrow definitions, there has been a failure in conceptualising topics associated with political risk. This resulted in companies ending up with the wrong results because they utilised the incorrect data in their analysis. As stated in the previous section, taking a risk will not always result in a negative outcome, there is the potential for a positive outcome. Lastly, it was argued that with too much focus placed on governmental policies and other political events the other causes of political risk are not considered (Alon & Martin, 1998:11).

Alon *et al.* (2006), in their writing identified that there were several ways in which it was possible to identify political risk that international companies could potentially face. These political risks are explained as follows “(1) prevalent legal rules and regulations within a given country; (2) war and security issues, (3) governmental economic and (4) fiscal policies; (5) the existence of trade barriers” and more (Alon *et al.*, 2006:625). Each of these factors has the potential to affect international companies operating within a country. However, Alon *et al.* (2006) argues that the impact of these political risk factors differs from company to company, depending on the sector in which they operate (2006:625). The risk of war (civil) or a terrorist attack will pose a greater risk to the oil and gas industry (Alon *et al.*, 2006:625).<sup>4</sup>

One of the best all round definitions of political risk many authors argue is the definition provided in Simon’s writing (1982). Simon states that political risk refers to the following: “the governmental and societal actions and policies, originating either within or outside the host country, and negatively affecting either a select group of, or the majority of foreign business operations and investments” (1982:68). In the article written by Alon and Martin (1998) and later Alon *et al.* (2006), both argue for the validity and the usefulness of Simon’s definition. Alon and Martin supported the definition by stating it was relevant because it took into consideration that international

---

<sup>4</sup> The financial sectors are far more concerned with the risks of balance of payments, changes in interest rates, hyperinflation and market liquidity, in their consideration in investing in a particular country. Alon *et al.* presented the example of the Brazil when their currency devaluated by 40 percent in 1999, which resulted in the International Monetary Fund (IMF) withdrawing from the country and creating an uninviting investment climate (2006:629).

companies from “the host-country environment, home-country environment, international environment and the global environment” (Alon & Martin, 1998, cited in Alon *et al.*, 2006:625). Alon *et al.* (2006) put forward three reasons in their argument for supporting Simon’s definition, even though the definition at that stage had been developed over twenty-four years earlier. They argue that the definition “(1) views political risk in the general environmental context, (2) differentiates between macro and micro risks, and (3) distinguishes between internal and external causes of political risk” (2006:625). Alon *et al.* (2006) does critique Simon’s (1982) definition as they extended the definition by adding an economic dimension. Alon *et al.* (2006) argues that an economic dimension is an important source of political risk, as economics and politics are often inseparable from one another. This is an important critique, as oil and gas companies often take into consideration economic factors with their political risk analysis because their focus is on maintaining their profit.

While many might consider Simon’s (1982) definition to be the best well-rounded definition some authors argue that this definition is no longer sufficient for political risk in the twenty-first century. Simon’s (1982) is no longer sufficient as when Simon wrote it, he could not have predicted the role that the growth of technology would play and the changes that would occur in political risk as a result. In the recently published book *Political Risk: How Businesses and Organisations Can Anticipate Global Insecurity* the authors, Rice and Zegart, address these inefficiencies and put forward a far more sufficient definition of political risk for the twenty-first century. Rice and Zegart in their writing do support the earlier authors’ definitions such as Robock (1971), Kobrin (1979) and Simon (1982), which view the government as being the main arbiter in the business environment (2018:14). While they support this perspective, they argue that the government is no longer the only important arbiter.

The authors state that technology such as cell phones enable citizens, customers and organised groups to galvanise action at local, state, federal and international levels. As a result, the environment of risk in and outside countries has grown to be complicated and messy with players overlapping and intersecting. Rice and Zegart identify five levels of action generating political risks: Individuals, local groups, national governments, transnational actors and supranational/international institutions

(2018:36-37). As such, Rice and Zegart put forward that political risk in the twenty-first century should be defined as “the probability that a political action could affect a company in significant ways” (2018:15-16). Rice and Zegart specifically chose to use the words political action in order to indicate the growing role of risk generators outside the traditional places such as capitals, army barracks and party headquarters. The risks generated by these actors are continually growing but Rice and Zegart identify ten major political risks, which face business and companies. The following is a list and summary of each of these risks:

1. Geopolitics: Interstate wars, great power shifts, multilateral economic sanctions and interventions
2. Internal conflict: Social unrest, ethnic violence, migration, nationalism, separatism, federalism, civil wars, coups, revolutions
3. Laws, regulations, policies: Changes in foreign ownership rules, taxation, environmental regulations, national laws
4. Breaches of contract: Governments renegeing on contracts, including expropriations and politically motivated credit defaults
5. Corruption: Discriminatory taxation, systemic bribery
6. Extraterritorial reach: Unilateral sanctions, criminal investigations and prosecutions
7. Natural resource manipulation: politically motivated changes in supply of energy, rare earth minerals
8. Social activism: Events or opinions that “go viral,” facilitating collective action
9. Terrorism: Politically motivated threats or use of violence against persons, property
10. **Cyber threats: Theft or destruction of intellectual property, espionage, extortion, massive disruption of companies, industries, governments, and societies.**

(Rice & Zegart, 2018:74-75).

A number of different definitions for political risk have been presented in this section. For the purpose of this research study the definition of political risk presented by Rice and Zegart’s (2018) will be utilised. Rice and Zegart’s definition will be used because their definition acknowledges the inefficiencies of older definitions to address the new political risk landscape in the twenty-first century. In addressing these inefficiencies Rice and Zegart introduce the political risk of cyber-threats, which is key to this



research study. Rice and Zegart state that, “political risk is the probability that a political action could affect a company in significant ways” (2018:15-16).

## **2.5 Macro and Micro Political Risk**

Political risk is divided into two subcategories: macro and micro political risk. When an unexpected change occurs within the political environment and has an influence on all foreign business within a region, is referred to as macro-political risk. Large-scale disruptive socio-political events such as revolutions, wars and changes to investment rules, which have an affect on all foreign companies within a country, are all examples of macro-political risk. This will generally occur when a country is going through periods of political unrest or different groups are targeting it across the political spectrum. A further division found within macro-political risk is that it can also be internal or external. Internal risk refers to risk posed by the domestic environment and external risk refers to the country itself or an outside company and even the global environment (Alon & Martin, 1998). In earlier literature Simon (1982) already critiqued this separation of internal and external risk. Simon (1982) instead argues that they should rather be combined, and political risk should be identified as being either society-related or governmental-related risk factors. Micro political risk is defined differently and is identified by different characteristics to that of macro political risk.

Change that only has an effect on specific industries or even specific companies is classified as micro-political risk (Robock, 1971:9). Kobrin argued in his writing that macro-risk is not the biggest political risk facing foreign companies, but rather that micro-political risks that have a greater effect on actual operations rather than overall ownership (1981:253). As was previously stated, Kobrin conducted a study that showed that expropriations were limited. Simon (1982) further argues that Robock’s (1971) differentiation between micro- and macro-political risks was crucial in indicating to both international investors and companies that they need to pay attention to the little changes that are industry-specific conditions, instead of the changes that come with more large-scale events which are perceived as catastrophic (Simon, 1982:66). Examples of micro-political risk, which the oil and gas industry face, were provided in Jakobsen’s (2012) research. According to Jakobsen these

examples are as follows: terrorist attacks against oil and gas installations, taxation increase aimed specifically at oil and gas companies, price controls for utilities and selective expropriation (2012:38).

The divide between macro- and micro-political risk is very much like the early division between authors on the matter of whether political instability or government intervention were the main political risk, according to Jakobsen (2012). Macro-political risk events tend to be those that are more eye-catching and have their own set of consequences. Micro-political risk events tend to be those that are considered less high profile and not as newsworthy. As stated previously, these micro-political risk events actually tend to occur far more frequently and have a higher impact on firms and result in greater losses. Even though the forms of macro-political risk, such as expropriation and mass nationalisation, are decreasing they still do exist. Though companies today face other risks now that fall under the concept of micro-political risk.

In the case of micro-political risk, Berlin, Berlin and Vrooman (2003), state that it can additionally be referred to as industry-specific risk or as a firm-specific risk. The distinction is important as it indicates how risk can differ from industry to industry. Lambrechts, Weldon & Boshoff (2010) argue that in the future there will predominantly be two factors that will have an influence on political risk. The first factor that will have an impact is when foreign-owned businesses hold a higher share in a country with increased micro-political risk there will be a greater level of change experienced in that industry (Lambrechts *et al.*, 2010:112). The second factor is that over time the local workforce will become more skilled providing them with a greater ability to run the companies successfully on their own which will essentially only lead to greater micro-risk (Lambrechts *et al.*, 2010:112). Micro-political risk is important to companies and will be further expanded on under the conception of industry- or firm-specific risk, which as stated is the other way of referring to micro-political risk.

Frynas and Mellahi provide an important critique that argues for the recognition that risk faced by companies varies from the type of company it is, the kind of project and

even the difference in the products that they produce (2003:542). Frynas and Mellahi's critique supports Kobrin's much earlier argument in his own writing in which he noted that political events have varied influence on different firms and different projects (Kobrin, 1982:40). Robock and Simmonds (1989) came to this same conclusion in their writing in which they were able to recognise that different businesses were sometimes impacted less than others by political risk. This was especially evident in their example of the political unrest that had occurred in El Salvador between the 1970s and 1980s. Earlier writing of Kobrin (1980) supports Robock and Simmonds, as his research was based on several companies where he found that the companies that were selected for expropriation were chosen because of the type of company that they were. Frynas and Mellahi further argue that it is necessary to recognise that investment decisions done through risk assessment are "highly project-specific and occasionally firm-specific or even product-specific" (2003:542). Even companies within the same industry, such as oil and gas companies, when experiencing the same political event might be affected differently.

Frynas and Mellahi confirmed this notion in the conclusion of their writing on their study of oil and gas companies in Nigeria (2003:558). Within their study, they found that the companies of Shell and Elf-Aquitaine, were able to handle potential political risks better than other companies as they were better equipped to deal with these potential risks (Frynas & Mellahi, 2003:559). Thus, they indicate that these two firms' willingness to invest in the region of Nigeria is best understood under their firm-specific risk or their overall ability to reduce the risk that they face. Critics have noted that industries such as oil and gas have little choice but to invest in high-risk locations as this is a common trend for extractive industries. The reason for industry-specific risk being prevalent in the extractive industry is as result of "growing nationalistic feelings and a conviction that natural resource endowments should be exploited for the welfare of all people in a nation rather than for profit" (Robock, 1971:10).

Another critique regarding firm specific risk was provided in Alon and Hebert (2009), in which they argued that there has been a lack of guidelines on how firms should approach an assessment of the specific risks that a specific firm could potentially face. Therefore, Frynas and Mellahi continue this argument and state that it is necessary for

scholars to continue to place more focus on the study of the branch of firm specific risk, rather than on the level of country- and industry-risk (2003:562). This argument of Frynas and Mellahi (2003) was supported in the later writing of Alon and Herbert (2009) who provided a similar critique, which stated that there was still far too little research that effectively covers the characteristic of firm-specific political risk.

Alon *et al.* (2006) worked to address this critique as their writing focused exclusively on the oil and gas sectors and the industry-specific risks that they face. Within their writing Alon *et al.* argue that one of the most sensitive sectors in which to invest in is the oil and gas industry (2006:631). Alon *et al.* (2006) are not alone in their statement that the oil and gas industry is the most sensitive investment sector. As the later writing by Lambrechts and Blomquist supports this statement in outlining that oil and gas companies are sensitive because of the fact that these natural resources are often perceived as being a country's national patrimony (2016:2). This sensitivity stems from the fact that the oil industry has the ability to produce wealth and power.

There are numerous risks that the oil and gas industry face that Lambrechts and Blomquist outline as follows: "corruption, taxation systems, governmental regulations, civil and labour unrest, political instability, environmental activism, repatriation restrictions, war, external threats and terrorism" (2016:2). Berlin *et al.* indicates that a reason for the heightened risk that the oil and gas industry faces is because they are predominantly located in unstable regions (2003:2). Berlin *et al.* (2003) estimates that roughly sixty-five percent of oil and gas reserves are located in the Middle East. This political instability does not hinder oil and gas companies from willingly exposing themselves to these risks, because as Alon *et al.* argue as long as they can manage this risk and still make a profit, they will accept this high-risk (2006:632). Following the September 11 terrorist attack in America, one of the predominant micro-risks that oil and gas industries face is terrorist attacks (Yetiv, 2011:193). The increase of attacks has resulted in a change in thinking about risk within the oil and gas industry. While terrorism did force a change in the thinking about risk in the oil and gas industry, another change in thinking is going to be needed. The threat landscape of the oil and gas industry is changing due to increased automation use making oil and gas vulnerabilities increasingly more vulnerable to the rising threat of cyber-attacks. Cyber-

attacks are predicted to be the biggest threat to face the oil and gas industry in the future as they replace traditional methods of terrorist attacks.

## **2.6 Risk Management and Risk Mitigation**

With a rapidly expanding global market a point of great concern for international companies and investors according to Lambrechts and Blomquist is that they need to take into consideration all of the political risks involved in their investment (2016:1). This is especially true of the oil and gas industry, as an extractive industry, they will never be free of risk. However, Alon *et al.* argues that the oil and gas companies are far more willing to be exposed to these risks if there is a way to effectively manage these risks and maintain their profits (2006:632). These findings support earlier arguments that the primary objective of oil and gas companies, when investing, is risk management (Miller, 1992:311). In more recent literature, Brink defines political risk management as follows: “the sum of the actions foreign investors or multinational corporations (MNC) take to try and keep at an acceptable level the degree or measure of investment risk associated with their activities” (2004:149). Years earlier Haendel (1979) provided a more well-rounded and in-depth definition. Haendel defines risk management as “identifying risks, assigning a value to them, anticipating losses, and making objective decisions about what steps to take before losses occur so that they have the least impact on the operations of the enterprise” (1979:135). Haendel’s definition of risk management follows the process of decision-making used by the rational man described at the beginning of this chapter.

It is through a company’s assessment of the different risk factors, which could have an effect on their investment, that decisions can be made on what mitigation measures they should take (Berlin *et al.*, 2003:6). Within Brink’s (2004) writing on political risk management, she distinguishes between two techniques: protective and integrative. Protective techniques seek to reduce the overall severity of a company’s loss and endeavour to ensure the protection of key internal strengths of an MNC (Brink, 2004:156). Integrative techniques are focused on “reducing the frequency of loss and their main aim is to influence relations with institutions and actors in the political environment” (Brink, 2004:156). Instead a well-rounded risk management plan will consist of both techniques as they each address a different aspect of a company. Berlin

*et al.*, puts forward two different ways in which to mitigate political risk: political risk insurance or what they term de facto insurance (Berlin *et al.*, 2003:6). Political risk insurance does not seek to prevent loss, instead it focuses on assuring investors that they will receive compensation for part or all of their investment if a loss does occur (Berlin *et al.* 2003:6). De facto political insurances seek to prevent losses from happening in the first place. These two methods of mitigation, are same as Brink's techniques, complement one another and are not mutually exclusive (Berlin *et al.*, 2003:6).

Within the literature there is recognition that while it is necessary to conduct political risk analysis and propose plans for management and mitigation prior to investment, it is not always done. This is particularly true within oil and gas companies. Often times, this analysis is conducted in response to an event that is already happening rather than continually conducting political risk management. Alternatively, risk forecasts are conducted at the request of investors who are looking to invest or increase their investment. As a result of companies not continually looking at risk management or updating their analysis, they often are only able to manage a problem after it has become apparent. One of the best-case studies of this occurred in 2013 with the In Amenas terrorist attack. The plant was a joint venture between BP and Statoil. Both companies did not publish the details of their security plans. Prior to the attack, a Statoil employee stated that the company considered political risk to be seen mainly as a public relations problem (Lambrechts & Blomquist, 2016:11).

A critique put forward by Lambrechts and Blomquist (2016) is that despite the number of political events that could affect the oil and gas industry there has still been a lack of effort in developing political risk management strategies. A critique put forward in the literature, before the one made by Lambrechts and Blomquist, was that many oil and gas companies continue to remain dependent on forecasting potential political developments (Lax, 1983:174). As was seen with Statoil prior to the In Amenas attack. The company lacked a holistic approach to their risk management. After the consequences of the attack become, did they initiate the creation of a political and security risk task force (Lambrechts & Blomquist, 2016:11). Oil and gas companies are incapable of simply moving where their production facilities are located. Following the

attack in 2013, it was realised that the biggest risk that oil and gas companies were going to face in the future is terrorism. As a result of the world economy's dependence on oil and gas, it makes the possibility of completely mitigating the threat of terrorism extremely difficult.

Even though it is not possible to completely mitigate the risk posed by terrorism, it is possible for oil and gas companies to manage this threat through “continuous evaluation [...] conducted before and during international operations” to make sure they are capable of addressing these changes” (Lambrechts & Blomquist, 2016:14-15). Finally, another important critique against risk mitigation and risk management is made in Lambrechts and Blomquist writing in which they state there still remains a rather limited amount of exploration conducted on how an increase of terrorist attacks affect the management and mitigation of risk (2016:4). Thus, it is necessary to continue to develop and expand on this literature but in order to do this, an understanding of cyber-threats and how they are changing is needed as well.

## **2.7 Cyber-Threats**

In order to understand cyber-threats, one first needs to understand the space in which these attacks are occurring. It is therefore necessary to look again at one of the driving forces of globalisation: the growth of the Internet. When trying to establish and explain the origin of the Internet begun as an internal experiment in the US military. Since its obscure beginning, the Internet has rapidly developed and grown according to Ahmad and Yunos it is now at the “centre of modern life and has become an important medium for business, economics, politics and communities” (Ahmad & Yunos, 2012:149). Ahmad and Yunos' observation on the Internet's development is supported in the writing of Negroponte, Palmisano and Segal, who state that the Internet can “transform commerce, create social and cultural networks with global reach, and become a surprisingly powerful vehicle for political organisation and protest alike...” (2013:ix). Evidence of the proliferation of the Internet is further evident in the statistics that the International Telecommunication Union (ITU) published in 2015. The ITU's statistics estimate that roughly “3.2 billion people are now using the Internet...” (ICT Data and Statistics, 2015:1). As the Internet has developed, Information and Communication Technology (ICT) has developed with it. The development of ICT has

resulted in there being “enormous gains in efficiency and productivity” (Ahmad & Yunos, 2012:149). This technological progress and infrastructure deployment has allowed the Internet to rapidly spread, which is only increasing in speed.

The growing interconnectedness has meant that in the 21<sup>st</sup> century we are rapidly moving towards a digital society. The pervasiveness of the Internet has brought changes, which are irreversible, to the global environment. According to the writing of de Borchgrave, Cillufo, Cardash and Ledgerwood this pervasiveness has brought with it the creation of “significant personal, organisational and infrastructural dependencies that are not confined by national borders” (2000:1). Despite there being many perceived benefits to the increased interconnectedness for the public, it has additionally brought with it the creation of numerous opportunities for those with devious motives to cause harm. These opportunities occur in the space referred to as cyberspace. While cyberspace is the arena where these events occur, there is still no standard or objective definition as to what it is.

The prefix ‘cyber’, is utilised to indicate a characteristic, which pertains to “information technology and the Internet in its capacity as an electronic communications network” (Hiralal, 2017:2). According to Choucri’s writing, cyberspace is defined as a “venue that allows users to engage in activities conducted over electronic fields whose special domains transcend traditional territorial, governmental, social and economic constraints” (2012:6). In defining cyberspace, Ahmad and Yunos’ indicate that those wishing to conduct cyber-attacks will utilise the cyberspace and ICT to their advantage (2012:149). Ahmed and Yonus’ are in agreement with Chourcri on the transcendent nature of it, as they state the following: “cyberspace has no boundaries” (2012:149). Thus, traditional borders, which distinguish one country from another, do not govern cyberspace, as it does not have these same boundaries. Ultimately, the Internet and cyberspace have brought inherent insecurities.

Inherent insecurities of the Internet and cyberspace provide contemporary terrorists and terrorist organisations, nation-states and people’s movements with the ability to utilise cyberspace and the wide range of opportunities it provides. According to Stohl, terrorists will utilise these opportunities in order to “support their campaigns of violence



and if they are proficient, significantly further their political objectives” (2006:229). While the concepts of crime and terrorism are considered to be traditional concepts and occur in the physical domain, the newest addition in this instance is the aspect of the ‘cyber’ domain. The convergence of the cyber domain and terrorism or crime is often referred to as cyberterrorism. Senior research fellow at the Institute for Security and Intelligence in California, Barry Collin, was the first to coin the term cyberterrorism in his writing in the 1980s (Gordon & Ford, 2003:3; Ahmad & Yunos, 2012:149-150; Denning, 2001:241). Collin, in defining the concept of cyber-terrorism, stated that the vehicle of cyberterrorism was formed from the convergence of the virtual world<sup>5</sup> with the physical world<sup>6</sup>. Collin’s definition of cyberterrorism may be the earliest definition but since the concept’s introduction numerous other authors have supplied numerous definitions.

Pollitt (1998), in his writing on cyberterrorism, combines Collin’s definition with the US Department of States’ definition of terrorism<sup>7</sup> in order to construct a definition of cyberterrorism. Pollitt (1998) provided the first working definition of cyberterrorism. Pollitt defines cyberterrorism as “the premeditated, politically motivated attack against information, computer systems, computer programmes and data which results in violence against non-combatant targets by sub national groups or clandestine agents” (1998:9). However, a problem with Pollitt’s definition is that it is very narrow. Pollitt argues that he kept his definition narrow in order to be able to differentiate from other forms of computer abuse.<sup>8</sup>

---

<sup>5</sup> Collin classifies the virtual world as being the arena where computer programmes are able to function and where data moves (Collins cited in Ahmad & Yunos, 2012:150).

<sup>6</sup> Collin defines the physical world as the place where society lives and functions (Collins cited in Ahmad & Yunos, 2012:150).

<sup>7</sup> The US Department of Defense (DOD), Federal Bureau of Investigation (FBI) and State Department define terrorism as the calculated use of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological (Lachow, 2009:438).

<sup>8</sup> Pollitt defines computer crime, economic espionage, or information warfare as other forms of computer abuse (1998:9).

This points to a weakness in Pollitt's definition, as these other forms of computer abuse start to be included in other authors' definitions, such as Lachow's (2009) which will be looked at later. Lewis, in his work on cyberterrorism, defined it as "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population" (Lewis, 2002:1). Lewis' definition, unlike Pollitt's, acknowledges the fact that the perpetrators are using the computer networks and the fact that they can be aimed at critical infrastructures. Lewis adds that nations and critical infrastructures are becoming more dependent on computer operations providing the premise for cyberterrorism. Ultimately this creates what Lewis refers to as a "massive electronic Achilles' Heel" (Lewis, 2002:1).

Alternatively, author Nagpal (2002) sought to examine cyberterrorism in the context of globalisation. In his examination he defines cyberterrorism as "the premeditated use of disruptive activities, or the threat thereof, in cyberspace, with the intention to further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives" (Nagpal, 2002:2). Another author whose definition is often utilised by others is Weimann's (2004a) definition of cyberterrorism. Weimann defines cyberterrorism as "unlawful attacks and threats of attacks against computers, networks and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives." (2004a:4). Rollins and Wilson state that in defining cyberterrorism there are at least two ways in which to do so. The first is effects-based and the second is intent-based. Rollins and Wilson (2007) define effects-based cyberterrorism as "when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism even if done by criminals" (Rollins & Wilson, 2007:3). Intent-based cyberterrorism is defined as existing "when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage" (Rollins & Wilson, 2007:3). Negpal, Weimann and Rollins and Wilson all acknowledge that cyberterrorism is utilised to intimidate governments or people through computer attacks to further political, ideological, social or economic objectives.

Stohl in his examination of the various definitions of cyberterrorism, argued that each of the definitions he has looked at “include[d] some form of intimidat[ion], coerc[ion], influence as well as violence or threat [thereof]” (2006:229). Stohl’s argument proves to be true in looking at the above-mentioned definitions of Rollins and Wilson (2007), Weimann (2004a), Negpal (2002), Lewis (2002) and Pollitt (1998). As previously mentioned, each of these definitions of cyberterrorism mentions the use of violence, threat of violence, influence and intimidation. Thus, Stohl utilises his finding in formulating his own definition of cyberterrorism and defines it as follows: “the purposeful act or the threat of the act of violence to create fear and/or compliant behaviour in a victim and/or audience of the act of threat” (2006:229). Stohl’s definition is a far broader definition, thus leaving a lot more open to interpretation.

The most widely cited paper on the issue of cyberterrorism is Dorothy Denning’s testimony before the Special Oversight Panel on Terrorism (Denning, 2000). Denning is considered to be a leading authority on the subjects of cyberterrorism and information warfare. In defining cyberterrorism, Denning supports the understanding that cyberterrorism is the convergence of cyberspace and terrorism, as was originally stated by Collins (Denning, 2000:1). Ultimately, Denning states that cyberterrorism is defined as follows:

It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, as an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. (Denning, 2000:1)

Denning adds to this overall definition of cyberterrorism and states that any cyber-attacks, which disrupt nonessential services or is merely a costly nuisance, are not considered to be cyberterrorism (Denning, 2000:1). Within her early research, Denning concluded at that time cyberterrorism did not seem to pose an imminent threat but still cautioned that this could easily change in the future (Denning, 2000:8). Denning additionally made note of the advantages that came with cyberterrorism, such as the

fact that it can be conducted remotely and anonymously (Denning, 2000:8). Denning's conclusion altered slightly as did her definition over the next seven years in the further research she conducted on the topic of cyberterrorism. Denning updated her definition of cyberterrorism, in her research, on the threat that cyberterrorism posed following the 9/11 attacks. Denning's updated definition of cyberterrorism states that it is defined as follows:

Highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction and disruption against digital property (Denning, 2007:124).

In conclusion to her updated analysis, Denning states that over the past couple of years terrorists have shown a growing interest in cyberterrorism and that it could start to pose a far more serious risk in the future (Denning cited in Lachow, 2009:451). The change in Denning's findings, in the space of a few years, indicates how rapidly the threat posed by cyberterrorism can develop and increase.

In later writing by Lachow (2009), he introduces one of the most important critiques to the utilisation of the term cyberterrorism. Lachow argues that the term cyberterrorism is often applied or misapplied to a wide range of activities (2009:439). Applying the term to a wide range of activities has resulted in cyberterrorism seeming to be the biggest threat. Lachow draws attention to the fact that when news articles utilise the term cyberterrorism it is not terrorist groups engaging in cyberterrorism but rather nation-states, hackers and criminals (Lachow, 2009:439). Lachow proposed that cyberterrorism is merely one method of cyber-attack, not the only one. Lachow (2009) suggests that there are rather at least five methods of attack and they should rather be referred to as cyber-threats. This idea is supported in the authors' earlier writing. An example of this is seen in Beggs' writing when he argues that one cannot confuse hacking with cyberterrorism, as they are two completely different things (2005:472). In the recent writing of Rice and Zegart, the authors utilise the term cyber-threats that they define as "theft or destruction of intellectual property, espionage, extortion, massive

disruption of companies, industries, governments, societies” (Rice & Zegart, 2018:75).

Lachow summarises these different methods of cyber-threats in the table below:

**Table 1: Cyber-Threats: Defining Terms**

	<b>Motivation</b>	<b>Target</b>	<b>Method</b>
<b>Cyber Terror</b>	Political or social change	Innocent victims	Computer-based violence or destruction
<b>Hactivism</b>	Political or social change	Decisionmakers or innocent victims	Protest via web page defacements or distributed denial of service (DDOS)
<b>Black Hat Hacking</b>	Ego, personal enmity	Individuals, companies, governments	Malware, viruses, worms, and hacking scripts
<b>Cyber Crime</b>	Economic gain	Individuals, companies	Malware for fraud, identity theft; DDOS for blackmail
<b>Cyber Espionage</b>	Economic and political gain	Individuals, companies, governments	Range of techniques to obtain information
<b>Information War</b>	Political or military gain	Infrastructures, information technology systems and data (private or public)	Range of techniques for attack or influence operations

Source: (Lachow, 2009:439).

Lachow defines hacktivism as the act of manipulating digital information for either politically or socially motivated purposes (2009:439). Hacktivism does not seek to create fear or a sense of horror. Decision-makers are generally the targets of hacktivism. Black hat hacking on the other hand is done with the explicit purpose of achieving a personal gain (Lachow, 2009:439). Cyber-espionage is defined by Lachow as the utilisation of “information technology systems to gather information about an organisation or society that is considered secret or confidential without the permission of the holder of the information” (2009:440). A wide range of actors such as groups, companies and nation-states can conduct cyber-espionage. In regards to the cyber-threat of cybercrime there is no widely accepted definition. However, most definitions of cybercrime, place their focus on the utilisation of networks or computers in facilitating crimes such as spamming fraud, data theft and child pornography. In defining the cyber-threat of information war, it refers to undisguised and offensive attacks by nation-states in order to deliberately disrupt or damage information and communication systems, which are Internet-based (Lachow, 2009: 444-445; Arquilla

and Ronfeldt, 1997:28-30). Despite identifying these different methods of cyber-threats, it is still easy for the boundaries between each of these methods still blur together. Additionally, it is of importance to note that a cyber-attack is not limited to using only one of these methods of attack at a time. It is therefore better to use the term cyber-attack when referring to a cyber-threat evolving into an actual attack. Thus, for the purpose of this research study Lachow's (2009) definition of cyber-threats will be utilised.

### **2.7.1 Cyber-Attacks**

Terrorist attacks by terrorist groups or organisations, against oil and gas companies have traditionally been carried out using physical methods. Terrorist groups attack through the use of weapons, bombs and infiltrating the oil and gas plantations, holding workers hostage and in the worst circumstances killing the plantation's workers. However, these methods of attack are slowly changing and being replaced. Physical terrorist attacks will not completely cease to be utilised but will continue to occur. The new rising trend of cyber-attacks will become the dominant method used in terrorist attacks against the oil and gas industry. The rising threat of cyber-attack was confirmed 27 years ago in the following statement: "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (National Academy of Sciences, 1991:7). Additionally, Statoil, an international energy company and the world's largest offshore operator, conducted a full risk assessment following the devastating attack at the In Amenas facility.

The purpose of this assessment was to determine if there was a future risk of such an attack occurring. Instead the assessment determined that cyber-security attacks would be the new long-term threat that oil and gas operations will face - not physical threats (Boman, 2015). In order to fully understand the threat that cyber-attacks pose it is necessary to look at the literature on cyber-attack's influence and whether it has an influence on specific industries. Additionally, it will be necessary to look at the operating systems within oil and gas companies and establish what the rapid development of technology has had an influence on. With technology rapidly developing industries are becoming increasingly digitalised and as such this puts them at greater risk of being infiltrated and hacked. The development of technology has led

to a push for more integration in the business environment and the oil and gas industries operating systems are no exception.

Within the oil and gas industry industrial control systems play a vital role. The industrial control system (ICS), Operational Technology (OT) Network, plays the largest role in automisation which consists of various industrial automation and control systems which are as follows: SCADA (supervisory control and data acquisition), DCS (distributed control systems), PLC (Programmable Logical Controllers), OPC (Open Platform Communications) servers, and other critical components (Polyakov, 2016). These OT automation and control systems are responsible for controlling and monitoring physical processes in the oil and gas industry. Ernst and Young published an assessment on the threat of cyber-attacks on the oil and gas industry that stated that cyber-threats to these OT systems could result in “production stoppages, a decrease in product quality or even destruction of infrastructure” (Ernst & Young, 2014).

Historically a majority of these OT networks have been isolated from the Internet and office networks through the use of air-gaped computers. This allowed for the OT systems to utilise proprietary hardware, software and communication tools in isolation from office networks and provided oil and gas companies with a strong protection against attacks. However, as time has progressed this level of protection has been removed as a result of the push for more business insight (Ernst & Young, 2014). This, combined with the “requirements for remote network access and the spread of hardware and software from traditional information technology (IT)”, such as Windows based platforms, has resulted in oil and gas companies integrating their control systems and their enterprise IT systems (Ernst & Young, 2014). All of which provides the oil and gas industry with greater flexibility but introduces a serious risk through an increased vulnerability through OT systems by providing a possible access point for cyber criminals to infiltrate networks and take control of the OT systems. The rise of cyber-threats and the creation of the vulnerabilities within the OT systems allow for cyber-attacks to be carried out against the oil and gas industry from a distance but still have just as devastating effects.



In Ernst and Young's assessment, they referred to the individuals that carry out these attacks as being hacktivists (Ernst & Young, 2014). These hacktivists are not concerned with the acquisition of company data but are rather seeking to create highly visible incidents that will embarrass or harm the companies involved in the oil and gas industry (Ernst & Young, 2014). These outcomes can be more visible in the manner of macro risk but remain a micro risk as cyber-attacks are industry specific. The outcome of a cyber-attack is dependent on the method of attack used. According to an article published by Forbes, if a cyber-attack is successful it can result in some of the following outcomes: plant shutdown, equipment damage, utilities interruption, production circle shutdown, inappropriate product quality, undetected spills and safety measure violation resulting in injuries and even death (Polyakov, 2017). These cyber-attacks could potentially be coupled with actual physical terrorist attacks to create even greater damage.

In an article published in the Pipeline & Gas Journal the top ten cyber-security vulnerabilities were identified as follows:

1. Lack of cybersecurity awareness
2. Remote work during operations and maintenance
3. Using standard IT products with known vulnerabilities in the production environment
4. A limited cybersecurity culture among vendors, suppliers and contractors
5. Insufficient separation of data networks
6. The use of mobile devices and storage units including smartphones
7. Data networks between on- and off- shore facilities
8. Insufficient physical security of data rooms, cabinets, etc.
9. Vulnerable software
10. Out-dated and ageing control systems in facilities

(Top ten cybersecurity vulnerabilities for oil and gas, 2016:26).

ABI Research expected that by 2018 oil and gas companies would be spending roughly US\$1.87 billion on cyber-security alone (Polyakov, 2017). Despite the predicted increased expenditure on cyber-security and the vulnerabilities identified, the oil and gas industry still fall victim to cyber-attacks because of a lack of awareness and



understanding. In a report published by the European Union Agency for Network and Information Security (ENISA), they confirmed in their key findings that there are just a few specialists, within the oil and gas industry, who have an in-depth understanding of cyber-security and the complexities of OT systems (European Union Agency for Network and Information Security, 2017). In their report ENISA also found that not that many companies within the oil and gas industry remain, which places the most importance on their physical infrastructure instead of the security of their computer process systems and data. This, despite the fact that oil and gas companies such as Statoil are starting to identify that cyber-attacks are going to be the greatest threat to the oil and gas industry. Lastly, the ENISA report highlights that there still is a lack of good practices identified to deal with this threat and there is a lack of visibility in terms of information sharing within the oil and gas industry (European Union Agency for Network Information Security, 2017). This falls in line with the fact that there is still currently a lack of academic literature that covers the risk management and mitigation of cyber-attacks against the oil and gas industry.

Despite the lack of literature on risk management and mitigation, cyber-attacks against the oil and gas companies have been occurring for a long time. One of the most prominent cyber-attacks against the oil and gas industry, thus far, occurred in 2012 when Saudi Aramco, Saudi Arabia's state-run oil giant, was hacked. Thirty thousand of Saudi Aramco's Windows-based computers were wiped clean by a self-replicating virus and was replaced by an image of a burning American Flag (Polyakov, 2016; Bronk & Tikk-Ringas, 2013:81). This attack had an effect on Aramco's business processes and some of the drilling and production data were lost. Aramco managed to clean the affected workstations and return to normal business, but it took roughly two weeks for Aramco to fully recover from this attack. The fact that the virus, which was dubbed Shamoon, was able to gain access to industrial control systems of the computers, which are involved in the drilling and refining operation, indicated how important it is for companies to utilise spare computers for business operations and the monitoring and controlling of the upstream and downstream sectors of oil and gas

companies' operations.<sup>9</sup> The Cutting Sword of Justice claimed responsibility for this attack and stated that they aimed to stop oil production and its flow into the international market because of the Al-Saud regime utilising Muslim oil resources.

While the attack on Saudi Aramco is the most prominent attack, it is not the only one. While physical terrorism generally takes place in politically unstable regions, it is possible for cyber-attacks to occur in regions that are not characterised by political upheaval, instability and conflict. Cyber-attacks can be conducted from great distances and do not require political instability to occur. Cyber-attacks are capable of attacking oil and gas companies in countries where there is political stability and relative peace, such as Norway. The second case occurred in 2014 where dozens of oil and gas companies in Norway were targeted by a cyber-attack, including Statoil one of Europe's biggest suppliers of energy. There is limited literature available on this event and it is mostly covered in news reports. Statoil was considered to be the main target of the attack (Leyden, 2014). However, the method used in the attack is unknown and the extent of the influence that the hack had also remains unknown (Bryne, 2014). Despite the lack of information available this attack is useful in showing that oil and gas companies in political stable regions are also likely to be targets of cyber-attacks.

## **2.10 Conclusion**

To conclude, this literature review sought to provide the conceptualisation and the key concepts in looking at risk mitigation and management of cyber-attacks against the oil and gas industry. The theoretical grounding of rational choice theory, problem solving and decision-making provided the understanding of how decisions and problems are made through rational thought in using the information available to them. The conceptualisation of risk, political risk, political-security risk, macro-and micro risk with the focus being on industry-or firm-specific risks helped to further develop an understanding. The literature that exists on risk management and mitigation and

---

<sup>9</sup> The upstream sector is in control of searching for potential underground or underwater crude oil and natural gas fields, drilling of exploratory wells, and subsequently drilling and operating the wells that recover and bring the crude oil and/or raw natural gas to the surface (Polyakov, 2016). The downstream sector is responsible for refining of petroleum crude oil and the processing and purifying of raw natural gas and marketing and distribution of products derived from crude oil and natural gas (Polyakov, 2016).

terrorism were also conceptualised and looked at in order to understand their significance to the oil and gas industry and also with the emergence in literature of the new trend of cyber-attacks to the oil and gas industry. In the case of risk management and mitigation, Lambrechts and Blomquist identified that there has been little effort put towards political risk management strategies.

Lastly, the conceptualisation of cyber-attack was provided in order to establish if there was literature that addressed risk mitigation and management of cyber-attacks against the oil and gas industry. This is a very new field of study and is still developing. As result, there was a lack of literature that specifically addresses risk management and mitigation of cyber-attacks against oil and gas companies. There are news reports that cover the attacks but despite this there has not been a lot of academic writing on the topic. Despite this, there is recognition within the literature that is available that cyber-attacks are going to become one of the biggest threats that oil and gas companies face. With the recognition of this threat there is a lack of understanding and people qualified to manage and address this threat. The vulnerabilities that exist within the oil and gas industry against cyber-attacks have also managed to be identified.

## **Chapter Three: Identifying Vulnerabilities to Cyber-Threats in the Oil and Gas Industry**

### **3.1 Introduction**

The aim of this chapter is to examine the influence cyber-threats are having on the oil and gas industry. By examining the influence of cyber-threats on the oil and gas industry this chapter will also seek to identify vulnerabilities that are indicators of risk. Identifying these vulnerabilities which put oil and gas companies at risk of being the target of a cyber-attack, is crucial to oil and gas companies being able to develop strategies or propose methods to manage and mitigate the risk of cyber-threats. In order to decipher the influence of cyber-threats on the oil and gas industry, this chapter will start off by looking at how technology, automation and the introduction of the Internet of Things (IoT). Looking at this facet of the oil and gas industry is crucial to understanding why this industry is vulnerable to cyber-threats as they are the source of the creation of these vulnerabilities. Following the development of this understanding of how these vulnerabilities were introduced into the oil and gas industry, the second section of this chapter will seek to answer the main question of this research study by identifying these vulnerabilities. Due to the vast and complex environment of the oil and gas industry in order to identify the vulnerabilities, the second section will be divided into the three sectors of the oil and gas industry: upstream, midstream and downstream. By dividing the second section into these three sectors it will help establish how within each sector different vulnerabilities to cyber-threats exist.

### **3.2 Automation and the Internet of Things (IoT) in the Oil and Gas Industry**

The utilisation of automation within different industries and companies is not a new concept. Automation started as far back as the 18<sup>th</sup> century during the industrial revolution, which saw machinery being utilised to reduce the need for human assistance. Automation has only increased and grown, as technology has rapidly improved, and is now being utilised in numerous industries such as the car automotive industry, electronics manufacturing, medical industry and the food industry. The oil and gas industry have been slower in moving towards automation. The oil and gas industry started feeling immense pressure around 2016 to move towards even more automation as a result of the industry facing a weak demand as well as low prices since

2014 and creating the need to cut costs (Clark, Abraham & Goyal, 2016: 1; Automation in Oil and Gas industry, 2018; Thomson, 2017). Automation in the oil and gas industry has existed traditionally through Industrial Control Systems (ICS) such as Distributed Control Systems (DCS)<sup>10</sup>, Supervisory Control and Data Acquisition (SCADA)<sup>11</sup>, Safety Instrumented System (SIS)<sup>12</sup> and Manufacturing Execution Systems (MES)<sup>13</sup>. Automation helps the industry to ensure safe and reliable conditions. Over the last few years, there has been an increased reliance on automation; reliance has actually doubled in the past decade alone (Automation in Oil and Gas Industry, 2018). One of the primary reasons for oil and gas companies increasing their reliance on automation is that it cuts costs.

As mentioned above, the oil and gas industry faced a weak demand and low prices during the period from 2014 to 2016 and thus needed to find ways in which to cut costs. This new market reality facing the oil and gas industry resulted in massive layoffs as well as facility closures and cutting costs in all areas that they could. Becoming more reliant on automation, allowed oil and gas companies to continue to complete the process without delay while being able to increase productivity within budget. Oil and gas companies are going to become increasingly reliant on automation. DNV GL, technical advisors to the Oil and Gas industry, support these findings as they concluded in a recent report that the future of technology in the oil and gas industry lies in automation and operating digitally (DNV GL, 2016:58). Automation is changing as the industry is starting to demand a more integrated system, which has multiple functionalities. Oil and gas companies are rapidly seeking to integrate robotics, analytics and IoT (Mittal, Slaughter and Zonneveld, 2017:2).

---

<sup>10</sup> DCS are instrumental to controlling the complex production process. DCS supervises and coordinates each of the various controllers used in a plant system.

<sup>11</sup> SCADA is a control system that uses computers, networked data communications and graphical interfaces for high-level process supervisory management. SCADA also makes use of peripheral devices such as programmable logic controllers (PLC) to interact with plant processes and machinery

<sup>12</sup> SIS are hardware and software controls that are used in critical process systems. SIS is primarily used in processing facilities such as refineries to provide protection.

<sup>13</sup> MES is a computerised system which is utilised in manufacturing to track and document the transformation of raw materials to finished goods.

IoT refers to the ability to connect any device which has an on and off switch to the Internet. IoT platforms would create the ability to integrate communications, sensing and analytical capabilities. The core enabling technologies of IoT have improved in the last five years and developed enough that it is now being widely adopted by different industries, including the oil and gas industry (Slaughter, Bean & Mittal, 2015:2). IoT platforms create the ability for every system and every plant, at every location to be connected to one another as well as enabling remote monitoring that helps limit the danger to workers. While the integrated systems of IoT may hold many benefits, such as increased connectivity and driving value creation, it still comes at a cost. Automation through integrated IoT systems is allowing oil and gas companies to become even more vulnerable to cyber-breaches.

As was stated in chapter 2, oil and gas companies have been targets of cyber-attacks for years already. In the last few years alone, the oil and gas industry has seen the nature, scale and severity of cyber-attacks evolve and dramatically increase. According to a study conducted by Symantec in 2015, 43 percent of international energy companies were successfully hacked (Deering & Sweeney, 2017:65). Ernst and Young published a report, which examined the rise of IoT and how it was changing the threat landscape of the oil and gas industry with the introduction of cyber-threats (Digitization and cyber disruption, 2017). Through information gathered by Ernst and Young the report was able to establish just how much more the oil and gas industry is affected by the introduction of cyber-threats in comparison to any other industry, which is displayed in Figure 1 below.

**Figure 1: Cyber-threats faced by the oil and gas sector as compared to all industrial sectors**



(Source: Digitization and cyber disruption in oil and gas, 2017)<sup>14</sup>

Figure 1 shows just how disproportionately the oil and gas industry is influenced in comparison to other industries. While forty-two percent of all other sectors are targets of cyber-attacks seeking to steal intellectual property or data the oil and gas sector, in comparison is the target of sixty-five percent of such attacks. As will be established in the next section intellectual property and data are a vital and expensive part of the upstream sector. Figure 1 identifies an issue that leaves the oil and gas sector vulnerable to the risk of a cyber-attack, which is out-dated information security systems or architecture. While this is a factor that would affect other sectors only forty-eight percent suffer from this while sixty-five percent of the oil and gas sector is influenced by this vulnerability. This figure acts to ultimately display an overall issue and that is the low cyber-maturity of the oil and gas industry despite statistics and findings such as those shown in figure 1.

<sup>14</sup> Spelling errors found in figure 1 could not be altered due to it being acquired from a secondary source which did not allow for editing.

While the oil and gas industry does have really low cyber-maturity, this maturity does tend to vary from sector to sector. Boards of oil and gas companies present a fairly limited strategic appreciation for the issue that cyber-threats pose. Specialists and researchers, who have a long history of working in both energy and cyberspace argue that oil and gas companies are struggling to keep up with defending their organisations from the more advanced methods of attack and new generation malware (Deering & Sweeney, 2017:65). The sheer size of the oil and gas industry is yet another factor which makes it difficult to secure against cyber-threats. Networks of pipelines, exploration and production and refineries can stretch across continents. Not to mention, each operation in the industry is made up of thousands upon thousands of automated systems and IoT devices. In contrast, a hacker merely needs to identify a small number of security flaws in order to successfully exploit a system. This is just one harsh reality facing the oil and gas industry in trying to secure itself against cyber-threats. On the other hand, some oil and gas companies are utilising out-dated networks, which were not designed to handle the new security challenges facing the industry. According to cyber-security consultants a large number of companies use networks run by Windows XP; a 2003 system that is no longer updated by Microsoft (Eaton, 2017a). Some companies are using even older versions of Windows operating systems and in rare cases a few oil and gas companies still utilise MS-DOS.<sup>15</sup> The utilization of out-dated networks indicates that some oil and gas companies are not taking cyber-threats, posed by old network systems and the influence that a cyber-attack can have on overall security, seriously.

It is clear that automation has already made the oil and gas industry vulnerable to cyber-threats and IoT has only exacerbated that vulnerability. Each value stream in the oil and gas industry, from upstream right down to the petrol pump in the downstream, possesses weaknesses that make them vulnerable to cyber-threats. It is important to look at each sector of the supply chain to establish which areas are targets due to their vulnerability, which form of cyber-threat would be used against it and what influence a potential attack could have on the sector. Figure 2 displays the flow of the different

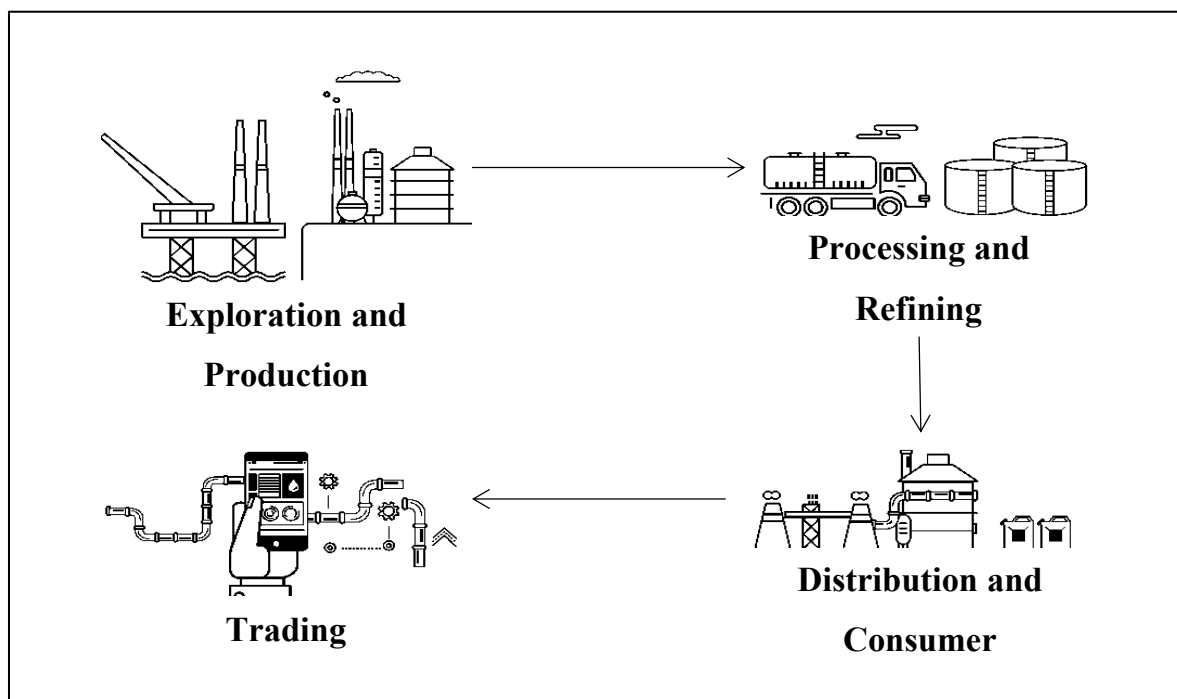
---

<sup>15</sup> MS-DOS is an operation system used by personal computers and developed in the 1980s. It acted as the precursor to Windows.



operations of the oil and gas industry in the value chain. Each of these operations falls under a different sector of the oil and gas stream. In order to identify the vulnerabilities, the next sections will look at each sector of the oil and gas industry individually in order to combat the complexity of the oil and gas industry. Each sector will start with a brief overview in order to understand the operations specific to each sector before taking a deeper look at identifying the vulnerabilities that are indicators of risk. This section of this chapter will start with the upstream sector as it is where operations of the oil and gas companies start.

**Figure 2: Flow of the operations in the Oil and Gas Industry**



(Source: The Cyber Security Threat to the Oil and Gas Industry, 2017).

### 3.3 Overview of Cyber-Threats to the Upstream Sector of the Oil and Gas Industry

Exploration and Production (E&P) or the upstream sector of oil and gas industry is highly vulnerable to cyber-attacks. According to research, conducted by Rick and Iyer, the upstream sector is considered to be the most vulnerable to cyber-attacks (2016:2). This vulnerability stems from the upstream sectors' status as critical infrastructure along with a complex ecosystem made-up of computation, networking and physical operational processes that are spread around the world (Mittal *et al.*, 2017:3). As a result, the upstream sector has a large attack surface with many attack vectors. Attack

surface refers to the total sum of vulnerabilities in any computing device or device which is accessible to a hacker. Attack vector refers to the path or ways a hacker will use in order to gain access to computers or network services to carry out an attack. Another factor that contributes to the vulnerability of the upstream sector is the contrasting priorities between an oil and gas companies' operation technology and information technology (IT) departments. These contrasting priorities create a clash of objectives in the upstream sector of safety versus security. Operation systems, especially those closest to drilling and well sites, have the priority of ensuring that devices such as sensors and programmable logic controllers can perform tasks, are available and can operate twenty-four seven. Thus, availability is their highest priority for operation technology followed by integrity and confidentiality. While IT systems focus on processes such as resource planning, their priority is confidentiality, while availability is the last. In other words, these two aspects have completely opposite priority focuses.

More security challenges face the upstream sector as a result of the technical setup of ICS. The technical setup stems from the fact that ICS are made up of different service providers, which use different technologies and have different IT security standards (Mittal *et al.*, 2017:4). Another issue, which adds to the diversity problem, is the life cycle of wells and ICS that make it very difficult to standardize, upgrade, and retrofit each of these systems frequently. With the introduction of connected technology, through using IoT and connecting the upstream operations in real time, the sector has opened an entirely new landscape of attack vectors for hackers. IoT systems are being utilised at field level and in doing so the upstream sector has taken cyber-threats right to the frontline of its operations. As the upstream sector is continuing to adopt these integrated technologies, it is ahead of the sectors' cyber-security abilities. This results in the upstream sector's core operation imperatives of safety for works, reliability of operations and creation of new value to be at risk due to the threat of cyber-attacks.

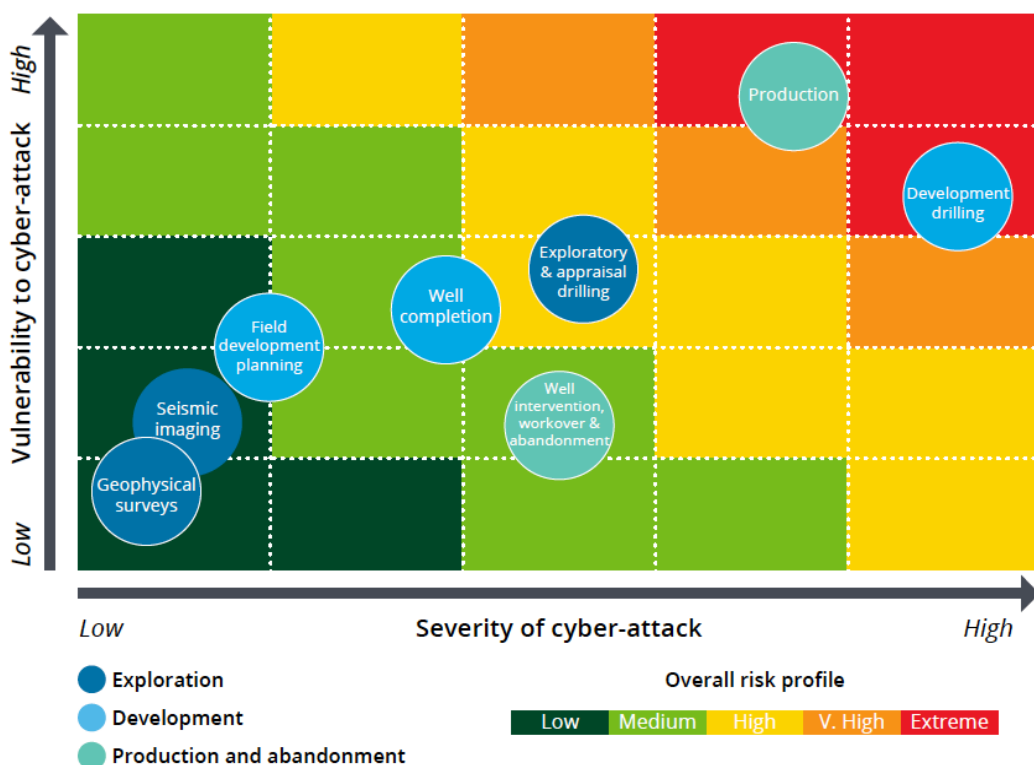
While everything discussed above provides a general perspective of the cyber vulnerabilities in the upstream sector, it is important to look at each of the different stages of the upstream sector (exploration, development and production). A focus on each stage will aid in identifying more clearly where vulnerabilities to cyber-threats

exist, as well as identify which operation in the upstream is the most vulnerable to cyber-threats. The vulnerabilities to cyber-threats in each industry need to be secured but identifying which stage is the most critical and risk prone stage will show companies where they need to start first. Figure three, pictured below, provides a basic overview of each of the operations in the different stages and their vulnerability to cyber-attacks and what the severity of these attacks could be. A more detailed analysis of figure three will be provided in the sections below. Identifying the vulnerabilities of each operation will aid in showing at which stage security needs to be prioritised. In general, identifying where the vulnerabilities exist is beneficial in helping to develop plans of managing and mitigating the threat cyber-attacks pose.

### 3.3.1 Identifying Cyber-threat Vulnerabilities in the Exploration stage

The exploration stage is made up of three separate operations: seismic imaging, geological surveys and exploratory and appraisal drilling. Vulnerabilities exist in each of these operations. Generally, the exploration stage in the upstream sector is ranked as having the lowest vulnerabilities to cyber-attacks and has a low severity impact as can be seen in Figure 3.

**Figure 3: Cyber vulnerability/severity matrix of upstream operations**



Source: (Mittal *et al.*, 2017:7).

The low rating of seismic imaging and geological surveys is the result of the fact that both these operations have a very simple ecosystem. The simplicity of their ecosystem stems from the fact that very few vendors are used in this stage, as the top geological vendors take up to fifty to sixty percent of the market and provide a wide range of services (Mittal *et al.*, 2017:6). Another factor, which aids in the low vulnerability in the exploration stage, is that these two operations have a closed data acquisition system. A closed data acquisition system means data captured about the rock formations is done through magnetics, geophones and hydrophones. The data captured by these devices is typically given to oil and gas companies through physical tapes or it is processed through propriety models. By sending physical tapes it keeps the data disconnected from being sent through e-mail, which would provide the opportunity for the e-mail to be hacked and the data stolen. The third operation in the exploration and production stage is exploratory and appraisal drilling, which in comparison to the previous two operations has a far higher risk profile.

Unlike the previous two operations, exploratory and appraisal drilling is considered to have a high vulnerability to cyber-attacks and the impact may have a high severity. Exploratory and appraisal drilling follows seismic and geographical surveys and its findings are key to an oil and gas company's decision on whether or not they will continue with exploration and appraisal activities. Exploratory drilling will try to see if there actually is a presence of oil and gas. If there is a presence, then appraisal drilling will follow. Appraisal drilling utilises delineation wells in order to determine the extent of the reserves and can take a few years to complete and is a costly process. The data obtained through appraisal drilling is further analysed to decide if it is economically viable for an oil and gas company to produce oil from the reservoir. If the reservoir is considered to be economically viable, models are built in order to determine the volume of the reserve that development drilling can access. This data forms oil and gas companies' competitive field data, which is very valuable and is the most vulnerable to

the risk of cyber-attack (Mittal *et al.*, 2017:6). An example of such an attack is that of the Night Dragon.

The Night Dragon was a cyber-attack, which was carried out over a period of roughly three years from 2008 to 2011 (Mittal *et al.*, 2017:6; Deering & Sweeney, 2017:65). Five major oil and gas companies, including ExxonMobil, BP PLC and Chevron, and other large oil companies were targeted in the attack. Hackers discovered vulnerabilities on the different firms' internet-facing websites and the attack took advantage of these vulnerabilities. Once the cyber-attack had gained access to the proxy server the attackers sought to disabled proxy-settings in order to gain access to specific files of interest (Mittal *et al.*, 2017:6). The files of interest were focused on proprietary information on operational oil and gas field production systems, financial transactions and the exploration and bidding data from oil and gas companies (McAfee Foundstone Professional Services and McAfee Labs, 2011:7). The attackers, in some instances, collected data on different SCADA systems. The methods and tools used in this corporate espionage attack were unsophisticated, which allowed them to go undetected. As a result, it aided in keeping the attackers from being detected by the standard security software and network policies used by the various oil and gas companies. Chevron eventually admitted to not having been aware of the successful compromises of their data systems (Deering & Sweeney, 2017:66). Insufficient cyber-security on the different companies' websites is what put these companies at a greater risk of cyber-attacks. The Night Dragon attack presents a challenge facing the oil and gas industry in their management and mitigation of cyber-attacks as it shows, despite having security software, it was still not enough to protect their data.

Another challenge identified by the Night Dragon attack is even though exploration operations are classified as having a low vulnerability to the risk of cyber-attacks it can still be a target of an attack. This means that even if an operation or sector is considered to have a low vulnerability it does not mean it is safe. As such even though oil and gas companies will seek to prioritise the most vulnerable operations, those with lower vulnerability will need to be just as much of a priority. Another factor to consider is that the relatively low vulnerability can change in the near future as oil and gas companies invest in new technology which will digitalise, store and process

information on a supercomputer (Mittal *et al.*, 2007:6-7). This will create a higher level of vulnerability to cyber-attacks in the exploration stage and will have a greater impact on an oil and gas company. The second challenge exploration operations put forward is the matter of attacks taking place and going undetected, as was seen in the Night Dragon attack. Being unable to detect attacks or on-going attacks hinders any oil and gas companies' ability to properly protect against them. Additionally, an inability to detect attacks will make creating risk mitigation and management plans even more difficult.

### **3.3.2 Identifying Cyber-threat Vulnerabilities in the Development stage**

Unlike the exploration stage, the development stage of the upstream sector has a higher exposure to cyber-threats. Figure 2 indicates that the process of developmental drilling has a very high to extreme vulnerability to cyber-attacks and the severity of an attack would be extreme. The vulnerability to threats, which face the development stage, are similar to those facing exploratory and appraisal drilling but it has a far larger cyber-attack vector (Mittal, 2017:7). The larger attack vector of the development stage is caused by a variety of factors such as its higher drilling activities and the complexity of having to monitor operations above and below ground. Additionally, the development stage has a vastly more complex ecosystem than that of the exploration stage. This complex ecosystem is made up of different engineering firms, equipment and material from various suppliers as well as drillers and service firms. The complex ecosystem creates vulnerabilities to the risk of cyber-attacks as each of the different firms, suppliers and vendors utilise different methods of security to protect their products. These factors merely ensure that it is even more difficult for oil and gas companies to create risk mitigation and management plans.

Originally it was the diverse interests and objectives of all the different stakeholders in the development stage that created one of the biggest challenges to operators in creating a single cohesive protocol regarding cyber-security. This challenge was coupled with systemic concerns regarding rigs and/or new devices being used that might already be infected with malware entering into this already complex and challenging ecosystem (Hsieh, 2015). The malware, which already exists in these rigs and devices, goes undetected due to the fact that oil and gas companies think there is nothing wrong with

new rigs or devices. However, cyber-security tests are not done on the rigs being built or even once they are completed only the normal routine functional acceptance tests (FATs) and site acceptance tests (SAT). This points to the lack of concern and awareness of the threat that a cyber-attack poses to the development stage and the oil and gas industry as a whole.

The lack of concern for and awareness of the threat regarding malware existing on rigs is the result of the belief that these systems were designed around an isolated network (Mittal *et al.*, 2017:8). The lack of concern and awareness given to the threat of cyber-attacks is another challenge facing the oil and gas industry in developing management and mitigation strategies to combat this new and rising threat. As well as being a challenge to the development of mitigation and management strategies, the lack of awareness and concern is one of the most significant vulnerabilities facing the oil and gas industry when it comes to cyber-threats. One of the reasons why these cyber-security tests are not run is that the oil and gas industries considered physical barriers to reaching rigs and the natural defence of miles of ocean (mainly in the case of offshore rigs) to be enough of a barrier to keep rigs safe from cyber-attacks. This natural barrier is no longer enough or rather the strength of its protection is being reduced. The introduction of real-time operations allows for data collected on an oil rig to be accessed from anywhere in the world. The ability to access these rigs from anywhere in the world has taken the barrier away for hackers making oil rigs vulnerable and putting them onto hackers' radars. The consequences of the removal of the natural barrier has already seen attacks on oil rigs occurring.

According to Wagstaff, in 2014 hackers managed to tilt an oil rig forcing it to be shut down (2017; Mittal *et al.*, 2017:8). Four years earlier, there was another incident involving a rig, which had been en route from South Korea to South America and was so riddled with malware that it was forced to shut down for nineteen days before the malware could be removed (Wagstaff, 2014; Mittal *et al.*, 2017:8). These attacks act as indicators that development operations need to find and/or create a more comprehensive plan in securing its operations from cyber-attacks. Companies operating in the oil and gas industry can no longer rely on traditional security plans or their traditional way of thinking.

### 3.3.3 Identifying Cyber-threat Vulnerabilities in the Production stage

The production stage of the upstream sector operates with the purposes of extracting hydrocarbons and separating the mixture of liquid hydrocarbons, gas, water and solids from one another. Production also requires the removal of the constituents, which are non-saleable, and the selling of the liquid hydrocarbons and gas. The production stage is considered to have the highest vulnerability to the risk of cyber-attacks out of all three operations in the upstream sector. Figure 2 indicates that production has an extreme vulnerability to cyber-attacks with a very high to extreme severity impact. The vulnerability of the production stage is mainly a result of the legacy assets that this stage uses. The legacy assets are older assets used in operations and were not created with concerns for cyber-security in mind as such they have had to be retrofitted and patched sporadically over the years (Mittal *et al.*, 2017:8-9). In addition to the vulnerability these legacy assets pose, there is also a lack of monitoring tools that exist on these networks. In 2017, it was estimated that of the forty-four percent of facilities, which operate offshore worldwide, less than half of these oil and gas companies use the necessary monitoring tools on their networks (Heidar, 2016). Only fourteen percent of these companies have a fully operational Security Operations Centre (SOC). Without a SOC it means that even if companies conduct monitoring twenty-four seven and there is not an experienced team in place to analyse the data essentially, this makes the monitoring taking place ineffective and acts to indicate another vulnerability facing the oil and gas industry: a lack of educated employees who know how to deal with cyber-threats (Heidar, 2016).

Another factor, which intensifies the vulnerability which cyber-threats pose to the security of oil and gas companies, is its expansive operation environment. This factor is exacerbated by the fact that the role of instrument vendors has changed from being system suppliers to system aggregators. In 2017, it was estimated that in the US alone there were over twenty-five thousand producing wells (Mittal *et al.*, 2017:8). Each of these twenty-five thousand rigs have their own diverse set of ICS'. A lot of the ICS systems come from different vendors, which means each one has been built with a different configuration of vulnerabilities (Black Hat Amsterdam: Oil and Gas cyber-vulnerabilities, 2015). Maintenance of the various ICS systems occurs at different



times. These varied maintenance schedules raise another aspect in which integrated systems create vulnerability in the oil and gas industry. While one ICS of an integrated system might have had routine maintenance to address vulnerabilities and made it more secure it can still be targeted by hackers gaining access through another part of the integrated system which has unaddressed vulnerabilities.

Burner Management System is the perfect example of how a system used in the both exploration and production operations in the upstream sector can be breached in a cyber-attack. In a presentation presented by Alexander Polyakov and Mathieu Geli, titled *Cyber-security for oil and gas industries: how hackers can manipulate oil stocks*, they stated that Burner management systems (BMS) are considered to be one of the areas that can be most easily manipulated by hackers. BMS performs vital safety functions in the process of separation of liquid hydrocarbons, gas, water and solids from one another. The main purpose of BMS is to allow and to ensure the safe-start-up, operation, and shutdown of the Fired Heater (Cybersecurity for Oil and Gas Industries: How Hackers Can Manipulate Oil Stocks, 2016). There are multiple risks, including the risk of an explosion if hackers were to gain unauthorised access to BMS. One of the easiest ways for hackers to attack BMS is to turn off the purge, which can burn and damage the equipment.<sup>16</sup> Turning off the purge can in a more severe case result in an explosion. BMS is merely one example of a system, in the production stage, being a target of a cyber-attack because of its inherent vulnerabilities.

### **3.4 Overview of Cyber-threats to the Midstream Sector of the Oil and Gas Industry**

There has been a lack of information regarding how cyber-threats affect the oil and gas industry, this is particularly true for the midstream sector operations. Very few reports exist on how operations in the midstream sector are affected by cyber-attacks. There is a reason for the lack of reports, as will be seen when it comes to cyber-threats to oil tankers. The midstream sector is also a very hard sector to define. This confusion in

---

<sup>16</sup> Following firing periods deposits of coal and/or oil need to be purged from the system in order to reduce the concentration of flammable gas in the system. It needs to be done to ensure that no ignitable mixtures can form.

defining the operations the midstream sector is responsible for stems from the fact that sometimes they can be included in upstream and downstream operations. Most commonly it is understood that the midstream sector is responsible for the collection and transportation of crude oil and natural gas from the upstream sector to the downstream operations. Once crude oil has been refined into its different products it can be stored at oil depots (also referred to as tank farms, installations or oil terminals). From the oil depot the midstream sector is responsible for overseeing that the refined products are distributed to downstream distributors and consumers. The midstream sector company usually transports oil through the use of pipelines, rail, barges, oil tankers or trucks. Each method of transportation used in the midstream sector faces its own unique vulnerabilities to the risk of cyber-threats. Each of the vulnerabilities need to be looked at individually as these cyber-threats can only be dealt with independently by the businesses or companies that are supplying the services of transportation and/or storage.

### **3.4.1 Identifying Cyber-threat Vulnerabilities in the Distribution Sector**

The infrastructure of pipelines has become increasingly more dependent on digital systems. This dependency has made pipelines a ripe target for cyber-attacks (Krauss, 2018). Control valves, pressure monitors and various forms of automated monitoring devices are used to observe these pipelines all of which are connected to wireless networks. In the US for example there is an estimated two and a half million miles of oil, gas and chemical pipelines, which crisscross the country. According to cyber-security expert Andrew R. Lee if one of the valves or pressure monitors is breached by a cyber-attack, delivery services could be disrupted or it could be far more catastrophic (Krauss, 2018). If pipelines are tampered with it could result in explosions, oil spills, or fires all of which would put property, the environment and human lives at risk. As pipelines are one of the main methods of transportation that connect the upstream to the downstream, if there is a disruption at an individual pipeline it has the potential to disrupt operations in both the upstream and downstream sectors. The vulnerability of pipelines to cyber-attacks has already been made evident in attacks such as were seen in Turkey.

In 2008 a pipeline exploded in Refahiye, Turkey. Investigators at the time determined that the explosion was the result of mechanical failure due to oversight of the Turkish government's supervisors. The Kurdistan Workers' Party (PKK), a pro-Kurdish militant group, with a history of pipeline bombings, claimed responsibility for the attack. Western intelligence agencies did not believe the PKK were actually capable of such an attack. Following further investigation, however it was reported in 2014 that the explosion was actually the result of a cyber-attack (Hsieh, 2015; Robertson & Riley, 2014). The investigation conducted by the US identified that the hackers behind the attack had breached the pipeline's surveillance systems and valve stations. The hackers had then shut down the alarms systems and super pressurised the crude oil inside the pipeline, which resulted in the pipeline exploding. Recently four of the US' natural-gas pipeline operators were forced to temporarily shut down their computer communications with their customers for a week due to a cyber-attack on a shared data network (Krauss, 2018). Despite the shut-down, the cyber-attack did not stall gas service during that time. The companies targeted stated that they shut down their communication with customers merely as a precaution. Nevertheless, it remained unclear if the hackers had actually managed to steal customer data or not. Oneok, Energy Transfer Partners, Boardwalk Pipeline Partners and Eastern Shore Natural Gas, all of whom are leaders in the pipeline industry all reported to have suffered from communication system interruptions.

When it comes to oil depots, they are typically located close to oil refineries or close to where marine oil tankers are easily able to offload their cargo. In comparison to other operations in the oil and gas industry, oil depots are relatively unsophisticated. In many oil depots the same types of tanks and pipelines in use have been used for a very long time. Utilising older equipment can at times pose more of a risk to cyber-attacks than newer equipment; the storage of oil at depots is no exception. At the StocExpo Europe conference it was put forward that the two biggest threats facing oil depots are ransomware and Denial of Service (DDos). Cyber-espionage is another threat facing oil depots and terminals because though some may think it irrelevant to the industry, hackers could still utilise programmes to manipulate and/or influence the stock market (Storage Terminals need protection against cyber-attacks, 2018). Hackers can do this through interfering with production processes. While oil depots may have remained

relatively unsophisticated there has been a greater degree of automation used within them than before. Tank inventory systems (TIA), Terminal management systems and tank management systems are examples of automation systems used at oil depots. TIA's collect data from tank gauging system, which has made the task of checking the inventory status at oil depots far simpler.

TIA's are also very vulnerable to cyber-attacks and if the management consoles are breached an attack will have the ability to change alarm settings for tank levels, the temperature of the tanks and the pressure in the tank. If these tanks are tampered with by hackers, there is the potential for plant sabotage or shutdown, equipment could be damaged, certain legal compliances could be compromised and the safety of works and the surrounding areas could be at risk. In the previous mentioned presentation *Cyber-security for oil and gas industries: how hackers can manipulate oil stocks*, Polyakov and Geli explained how hackers could gain control of TIA's to the point where it was possible for a hacker to steal oil from a storage tank but the level shown in the tank gauge system would not change to indicate the decreased level of oil (Cybersecurity for Oil and Gas Industries: How Hackers Can Manipulate Oil Stocks, 2016). If hackers did this it would decrease the supply of oil and result in oil and gas companies losing a portion of their profit revenue.

Oil tankers are another method of transport when it comes to moving unrefined crude oil from their extraction points in upstream operations to downstream refineries. Much like other operations throughout the oil and gas industry oil tankers have also turned to and started utilising technology in order to help improve production, costs and also reduce the delivery schedules (Wagstaff, 2014). Oil tankers according to research have significant holes in three key technologies which sailors use in order to navigate, which makes them vulnerable to the risk of cyber-threats. These three technologies are Global Positioning System (GPS), marine Automatic Systems (AIS), and a system used for viewing digital nautical charts called Electronic Chart Display and Information System (ECDIS). While these technologies have been identified as being vulnerable to cyber-attacks there have yet to be any known reports of them been compromised by hackers.

According to maritime cyber-security experts, companies or businesses who own the oil tankers often do not want to report if a cyber-attack has occurred as they do not want to alarm their investors, regulators or insurers (Wagstaff, 2014). As such there are very few reports that exist on hackers having compromised maritime cyber-security. An example of companies' and businesses unwillingness' to report attacks can be seen in a report published by the IT company Panda Security in 2015 titled *Operation Oil Tanker: The Phantom Menace*. The hackers utilised what is referred to as legitimate tools with self-made scripts, which allowed them to bypass the warnings that antivirus software would detect. This reaffirms the fact that traditional security software is not sufficient in protecting the oil and gas industry from cyber-threats.

While the attack first appeared to be a non-targeted attack upon further investigation it was determined that it was actually a systematic and targeted attack against this specific sector of the oil and gas industry (Operation "Oil Tanker": The Phantom Menace, 2015: 7). Some believed that the purpose of the attack was to steal information and credentials, which the hackers could use to defraud oil brokers. The report, however, concluded that while the attack was targeted at oil tankers the object of the attack still remains unknown. Panda Security identified that a dozen or so companies had the system compromised by the cyber-attack. Yet none of these companies were willing to come forward to report the breach of their systems because they were unwilling to risk global attention on the vulnerabilities found in their IT security networks (Operation "Oil Tanker": The Phantom Menace, 2015). The unwillingness to share such information poses a challenge to security companies wanting to help mitigate the influence of cyber-attacks.

### **3.5 Overview of Cyber-threats to the Downstream Sector of the Oil and Gas Industry**

The downstream sector consists of a wide number of operations and processes. It makes up two sectors of the value chain of the oil and gas industry. The first sector is processing and refining and the second is the trading sector. The pipelines, refineries and tank farms located in the downstream sector all utilise ICS in order to maintain smooth and safe operations (Shattuck *et al.*, 2017:3). This has led to there being a long history of automation, which has provided the downstream sector with a higher level

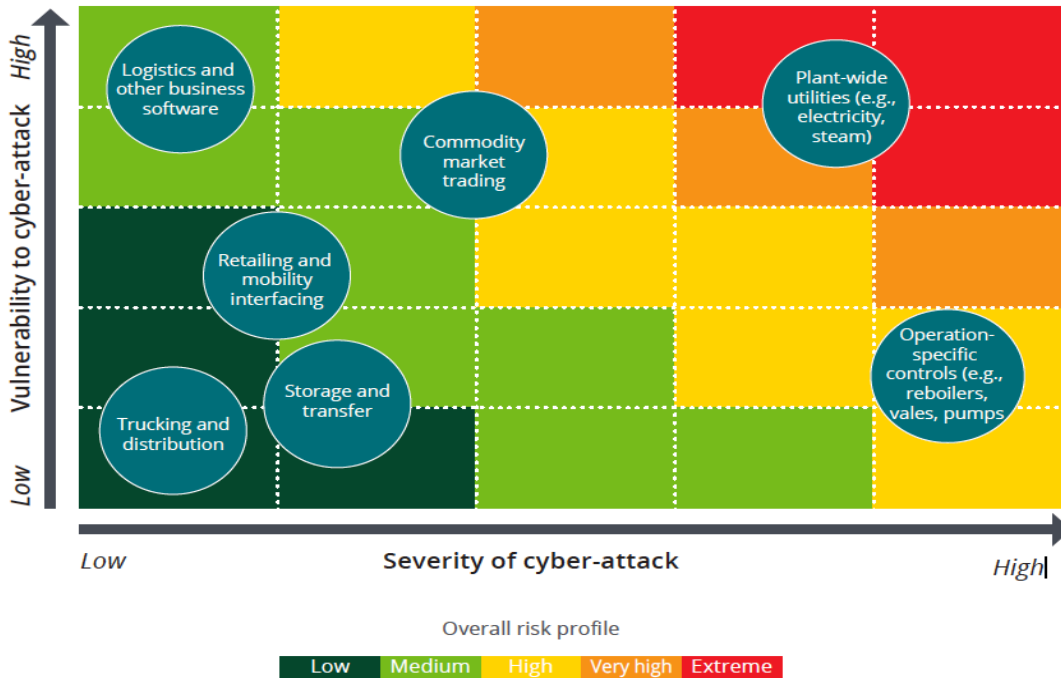
of maturity when it comes to monitoring the risks of cyber-threats to these systems. The higher level of maturity in monitoring of risk in the downstream sector could be challenged with the new pressure placed on the sector with the introduction of new areas of optimisation and starting to extend the value of the sector beyond the refinery. This pressure stems from the previously mentioned slow growth of demand for oil and gas, which has affected the industry as a whole.

As a result, new sensor technology, processing power, and remote operational capabilities are starting to be introduced into the downstream operations. In addition to these new technologies, IoT technology has also started to be introduced to the downstream sector. IoT technology will help the downstream sector unlock new value, which will be done by “eliminating redundancy, increasing uptime, and more promptly allocating feedstock, plant utilities, and products, while reducing costs” (Shattuck *et al.*, 2017:3). While IoT does come with many benefits it does bring with it new challenges to security as it makes the sector vulnerable to cyber-threats.

A report published by Deloitte examined the downstream sectors’ vulnerability to cyber-threats. The report determined that the downstream sector, as a whole, has a far lower level of vulnerability to cyber-attacks in comparison to the upstream sector operations (Shattuck *et al.*, 2017:4). While the report made this determination, it does not rule out the fact that vulnerabilities to cyber-threats still do exist in the downstream sector. As such, it is still important for oil and gas companies to consider the probability of a cyber-attack and the influence one could have. Figure 4 shows the level of vulnerability to a cyber-attack and the level of influence that an attack could have on different processes and operations in the downstream sector. Figure 4 also shows why the downstream sector is classified as having a low vulnerability to cyber-attacks. The risk is very unequally distributed as a majority of the operations in the downstream sector are clustered as having a low to medium vulnerability to cyber-attacks and for any cyber-attacks to have a low to medium impact. On the other hand, plant wide utilities have a very high to extreme vulnerability to cyber-attacks and can have a very high to extreme impact. Despite being perceived as having a low vulnerability, the opposite can still be argued. Companies operating downstream assets will still have a high potential and high frequency of cyber-threats. While figure 4 provides a road map

to looking at the cyber vulnerability in the downstream sector the findings are subject to change as the findings are gathered from a specific number of groups and are a snapshot of the time period that this research was conducted.

**Figure 4: Cyber vulnerability/severity matrix of downstream operations**



Source: (Shattuck *et al.*, 2017:6).

As in the other sectors, the downstream sector has operational controls, and as figure 4 shows they have high vulnerability to cyber-threats, which can have a high impact. This ranking stems from the fact that these operational controls are vulnerable to manipulation and can have the same physical and financial impacts as the upstream and midstream sector (Zonneveld & Slaughter, 2017:6). The downstream sector has not seen the introduction of many new technologies into its system, which means its security protocols have rarely needed to change. If a cyber-attack were to occur in the downstream sector the possible influences that could be felt are a loss in revenue, their brand could be damaged and/or there could be regulatory and compliance violations (Zonneveld & Slaughter, 2017:6). New operational systems are being introduced and are creating new vulnerabilities to cyber-threats in the downstream sector. These vulnerabilities stem from the fact that these systems are creating a far more complex

ecosystem, which as discussed previously, is an issue which makes it very hard for companies to develop mitigation and management strategies.

This overview has provided a very brief insight into the vulnerability to the cyber-threats facing the downstream sector. This overview does however, help confirm that vulnerabilities in the downstream sector exist but does not clearly define them. The following sections will focus on the two sectors in the oil and gas, refining and processing sector and the trading sector. It is important to look at each of these sectors individually as both of them are made up of very different operations and as such will have different vulnerabilities to cyber-threats. This is true for the entire oil and gas industry and ultimately each sector will need to develop individual plans to manage and mitigate the cyber-threats. As has been shown through this chapter a one size-fits-all cyber-security approach will not work in the downstream sector.

### **3.5.1 Identifying Cyber-threat Vulnerabilities in the Processing and Refining Sector**

The basic operations of the processing and refining sector entail the transformation and refinement of crude oil. Crude oil requires processing and refining because without refinement it essentially has one use, burning for fuel. The refining and processing of crude oil produces many different petroleum products, the focus is largely placed on the conversion of heavy fuel oil into gasoline, diesel, jet fuel and other fuel. There are many companies engaged in the refining and processing sector, which include oil refineries, petroleum product distributors and petrochemical plants. While the whole oil and gas industry is margin-driven, this is particularly true for the downstream sector. If a single day of operations is lost in 100,000 barrel-per-day refineries for example, revenue will be reduced by an estimated US\$ 5.5 million and profit by US\$1.4 million (Shattuck, Slaughter & Zonneveld, 2017:4). Cyber-threats are placing these operations at risk even using traditional methods of operation, especially since the introduction of technology.

Traditionally manual valves have been used along with safe design practices that have reduced the risk posed by cyber-threats. While it might reduce the risk of cyber-threats it does not completely remove the risk, as there is still a level of vulnerability that exists.



Processing and refining operations can continue to use manual valves and safe design practices to keep the risk of cyber-threats down but doing this will be at the expense of efficiency. As has been established, the processing and refining sector is margin-driven and thus will not sacrifice the efficiency provided by new technology over slower manual valves. An example is new sensors that are being introduced into the processing and refining sector. The sensor brings many benefits in value creation and efficiency, but it introduces new vulnerabilities to the risk of cyber-threats. Each sensor and the point where these new sensors are connected to monitor represent a new potential attack surface (Shattuck *et al.*, 2017:5). If a hacker successfully hacks a sensor on a pipeline, the hacker has the ability to alter the readings of how much gas is running through, change the pressure of the flow in the pipeline and even tamper with the heat of pipelines. Any of these alterations can result in either damaged equipment, which could potentially lead to millions or billions of US dollars to repair or put a halt to operations. This presents a dilemma for the oil and gas industry as automation through new technology is the way forward and they cannot sacrifice efficiency to decrease this risk. Essentially, this indicates that in order to continually produce efficiently oil and gas companies will need to be willing to accept a higher level of risk associated with these new technologies.

In 2017, a large oil refinery in the US hired the Minnesota based company RedTeam Security. RedTeam Security was hired for the specific purpose of testing the refinery's defences against cyber-attacks (Eaton, 2017b). The first member of the team stood just beyond the fence line of the refinery and swung a rubber mallet into the dirt. This was done in order to try and produce vibrations, which would distract the refinery's ground-penetrating radar system. The first member did not have to do this for long as a passing train provided the necessary cover for the rest of the team. What is concerning is that such a security method, which is considered a highly sophisticated form of security, could so easily be breached through simple methods. A further two members emerged and threw wool blankets over the barbed wire fence and climbed over it and made their way towards a small building which housed the facility's computer controls. The team had expected to have to hack the electronic lock that had been installed to prevent lock picking. They had stolen and cloned badges of employees of the refinery to deal with the electronic lock. The fact that the members of this security had so easily been able

to steal employees' badges, without them noticing, is concerning as it again points to a lack of vigilance and awareness amongst employees about cyber-threats. It also indicates how cyber-attacks are not merely limited to malicious malware attacking a system.

Despite acquiring these badges, the team actually found they did not need them. The door no longer sat properly in its frame creating just enough space that the team could just shimmy it open. The fact that a high-tech device meant to make the facility more secure, was easily manipulated physically due to lack of maintenance and is reason for concern. Ultimately, this indicates that oil and gas companies cannot become overly reliant on high-tech security methods as they can easily be circumvented in attempts to gain access to facilities' controls in a cyber-attack that is combined with physical penetration of a facility. After the team had gained access to the control room, the team planted a small device roughly the size of a credit card. The device began penetrating the refinery control systems giving the team control of the industrial control systems. The team was able to breach the refinery's system with only a couple of hundred dollars' worth of gear (all of which had been bought on Amazon) without anyone being aware of the attack (Eaton, 2017b).

The easy success that RedTeam Security had, presents a stark reality when looking at the cyber-attacks of the processing and refining sector. If this attack had been real, the implications would have been devastating. While many might think or hope that the success of this test was an exception it is not. In other private tests conducted by other private specialists there have been numerous successful cyber-attacks of valves, pumps and pipelines (Eaton, 2017b). Jason Larsen, a leader of a security team at IOActive states that whenever they conduct tests, they always gain access and often without being detected. The success of these tests indicates that refineries are actually one of the most vulnerable targets of cyber-attacks in the oil and gas industry, which appears to be due to a lack of awareness surrounding the sector's vulnerability to cyber-attacks.

### **3.5.2 Identifying Cyber-threat Vulnerabilities to the Trading sector**

Identifying and examining vulnerabilities to cyber-threats to trading operations is far more complex than with any of the other operations previously discussed. Often when

one considers cyber-threats to the trading sector, the immediate thought is petrol/gas stations. This assumption is not entirely wrong. Trading operations of the downstream sector do deal directly with customers, such as at petrol pumps. The direct interaction with customers creates the opportunities for hackers to steal customer information, such as their credit card information. Hackers have for a long time stolen the financial information of drivers through the use of credit card skimmers (Morris, 2018). A credit card skimmer is a small electronic device which hackers install inside card readers at self-servicing petrol pumps. The stolen information is sent back to the hacker via Bluetooth. Credit card skimmers are typically undetectable to consumers. The use of credit card skimmers was particularly evident last year in the US. Credit card skimmers have become a rampant issue, which saw the US Secret Service going to over eighty locations in twenty-one states to find credit card skimmers at gas stations. In their search, they found roughly fifty-nine credit card skimmers (Shoot, 2018). The Secret Service estimated that millions of dollars were stolen from consumers at gas stations as a result of credit card skimmers. While credit card skimmers are a method of cyber-attacks on oil and gas companies, it is mostly consumers, not the oil and gas companies that feel the impact. However, if credit card skimmers are found at a particular gas station it has the ability to damage the reputation of the company. Damage to an oil and gas industry reputation can result in less consumers utilising their stations to buy gas, which can result in a loss of revenue.

Credit card skimmers are not the only vulnerability to cyber-threats facing gas stations. Another vulnerability in trading operations at gas stations is the rise of cyber-attacks aimed at stealing gasoline from petrol pumps. Petrol pump systems are vulnerable to cyber-attacks because they are Internet facing systems and have no security measures in place to protect against cyber-threats. The vulnerability of pump systems first arose in 2015 when a pump monitoring system in the US was modified by a hacker (Wilhoit & Hilt, 2015). The hacker, who investigators suspect of being affiliated with the group Anonymous, merely changed the name of the pump. While there might not have been any major impact from the attack it did draw hackers' attention to the vulnerability of petrol pumps. Security experts have since continued to warn gas stations of the vulnerability of gas pumps to hackers, which has largely been ignored by oil and gas

companies. This once again is due to the lack of concern given to the threat by those in senior positions in oil and gas companies.

The lack of concern is evident as last year a petrol pump in the US was breached by hackers and it resulted in 600 gallons of gas being stolen from the gas station. The loss of the 600 gallons gas resulted in the gas station losing US\$ 1,800 of revenue which was the estimated value of the gas (Morris, 2018). No details on the technical aspects of the hack have been reported only that an attendant at the station was unable to turn off the pump using the normal methods. Another attack occurred when an employee at a BP gas station manipulated the gas pump computers, which allowed him to steal roughly US\$ 300,000 of gas over a three-year period (Morris, 2018; Grom, 2018). The BP station became aware of the hack when they started to notice that the amount of fuel being delivered to the station and the number of sales did not add up. The company originally thought the discrepancy was due to mechanical problems, underground storage leaks or equipment issues (Grom, 2018). When each of these possibilities were ruled out computer diagnostic tests were run which then revealed the manipulation of the gas pump computers. Successful cyber-attacks result in large loss of revenue to oil and gas companies that cannot be overlooked.

While it is clear that trading operations face their own unique vulnerabilities to the risk of cyber-threats, such as petrol pumps being targeted, it is worth noting that trading operations have the ability to suffer from the influence of cyber-attacks to other sectors. If a cyber-attack on a pipeline transporting oil results in an explosion this will result in shortage in supply which could result in a loss of revenue for distribution companies. The business or company, who bought the oil, will suffer from a loss of revenue as they will need to buy more oil to replace the oil lost in the explosion in order to avoid a lack of supply.

### **3.6 Vulnerabilities to Cyber-threats Identified within the Oil and Gas Industry**

As was outlined in the introduction of this chapter one of the key purposes was to identify vulnerabilities to cyber-threats in the oil and gas industry. Identifying these vulnerabilities is an important step towards developing and putting in place protocols, which can help mitigate or manage cyber-threats. Through looking at each sector in the

oil and gas industry and their different operations individually, various vulnerabilities were identified. While a hand-full of vulnerabilities was identified in the different sectors, ten of these vulnerabilities were ones that affected every sector of the oil and gas industry. While all the vulnerabilities identified are very important these ten vulnerabilities can be considered the most concerning as they are not limited to one sector. These ten key vulnerabilities to cyber-threats in the oil and gas industry identified in this research study are summarised in the table below.

**Table 2: Top Ten Vulnerabilities to Cyber-threats in the Oil and Gas Industry**

<b>Vulnerability</b>	<b>Explanation of Vulnerability</b>
Low cyber-maturity of the oil and gas industry	Due to the fact that cyber-threats are a new vulnerability facing the oil and gas industry companies do not have well-developed plans to deal with the risk and in some cases no plans have been put into place.
Lack of boardroom buy-in	Board members of oil and gas companies' limited acknowledgement of the risk posed by cyber-threats has resulted in the industry not taking the threat seriously.
Size of the oil and gas industry	The size of the industry makes it difficult to secure all the different automated systems and IoT devices being used in various operations.
Utilisation of out-dated and legacy assets	Oil and gas facilities using out-dated and legacy assets find themselves vulnerable due to the fact that they are not designed to deal with cyber-threats
Complex ecosystem	Through the use of different firms, suppliers and vendors, which use

	different security systems to protect their assets, it becomes a complex environment to secure.
Reliance on traditional methods of security	Reliance on traditional methods of security, such as natural barriers and standard virus detection software, makes oil and gas companies vulnerable to cyber-threats.
Reputational Risk	Oil and gas companies, which have a reputation as being a large source of revenue to their local government, are highly vulnerable to cyber-threats. Due to this reputation nation-states or other groups can target these oil and gas companies to destabilise their government's economy.
Lack of monitoring to detect cyber-threats	Oil and gas companies do not have any programmes or methods of monitoring for cyber-threats operating on their systems. Without having methods to monitor for cyber-threats, companies run the risk of having a cyber-attack going undetected for years.
Uneducated Employees	Employees, who are uneducated or not trained to deal with cyber-threats, results in them not being equipped to deal with an attack and they therefore lack overall awareness and vigilance.
Unwillingness to share information about their experience with cyber-threats	Oil and gas companies' unwillingness to share information about their experience creates a lack of awareness and concern about them in the industry as a whole.

(Compiled by author for this study).

While these are not the only vulnerabilities to cyber-threats at present, they are a key starting point for oil and gas companies when it comes to securing their facilities. However, political risk is constantly changing and evolving and that is particularly true of the political risk of cyber-threats. Cyber-threats are constantly developing, evolving and becoming more sophisticated at a rapid pace. As such, the vulnerabilities to cyber-threats found in the oil and gas industry will change and evolve just as rapidly. The table above will thus have to evolve with these changes.

### **3.7 Conclusion**

The aim of Chapter Three was to identify vulnerabilities to cyber-threats, which exist throughout the oil and gas industry. This chapter established that the oil and gas industry has opened themselves up to the risk of cyber-threats through the increased use of automation, technology and IoT. Despite the increased vulnerability very little awareness about the rising threat of cyber-attacks exist in the industry. In order to identify vulnerabilities of risk to cyber-threats each of the three sectors of the oil and gas industry were looked at individually. Each of the operations in the different sectors possess their own unique vulnerabilities due to the different forms of technology used in the different operations. Additionally, this chapter showed that each of the sectors in the oil and gas industry would experience different levels of severity should they be the target of a cyber-attack. One of the key observations of this chapter is just how complex the threat of cyber-attacks against the oil and gas industry are. This complexity points to oil and gas companies not being able to mitigate the threat of cyber-attacks and thus only manage the threat they pose. The political risk of cyber-threats is only going to change and develop at an increasingly rapid pace posing as a greater threat to oil and gas companies in the future. Cyber-attacks on oil and gas facilities, whose revenue certain governments are reliant on, can result in losses of revenue which can result in political upheaval in the country.

Chapter four will examine the selected case studies of this research. This examination will start with the cyber-attacks on the oil and gas company Saudi Aramco in Saudi Arabia. Specific focus will be placed on the first cyber-attack, which took place in 2012 and second attack, which occurred in 2017. Following this the second case study, the

cyber-attack on oil and gas companies in Norway will be examined. In the examination of the two case studies, Chapter Four will utilise the information provided in this chapter together with the theoretical and contextual foundation from Chapter Two to analyse them.



## **Chapter Four: The Influence of Cyber-Threats on the Oil and Gas Industry**

### **4.1 Introduction**

Chapter Two provided the theoretical foundation of this research study, while Chapter Three built on this foundation and sought to identify vulnerabilities to cyber-threats throughout the different sectors of the oil and gas industry. Hackers can exploit the identified vulnerabilities in order to gain access to facilities through different methods; ten key vulnerabilities were outlined and defined in Table 3.1. Chapter Four will utilise the information provided in earlier chapters to answer the research question of whether or not cyber-threats increase the risk faced by oil and gas companies. It will also look at one of the sub-research questions of how the oil and gas industry can utilise the vulnerabilities identified to either mitigate or manage the risk of cyber-threats. In order to do this, Chapter Four will be divided into three sections.

The first section of Chapter Four will analyse the cyber-attacks carried out against Saudi Aramco starting with the Shamoon attack, which is considered to be the biggest cyber-attack to have been carried out against an oil and gas company. This will be followed by Triton attack on a Saudi Aramco petrochemical facility, which happened in 2017 and is one of the most recent cyber-attacks. This section will examine the events of the attack, how the company was influenced and what the overall influence of the cyber-attack was on the oil and gas industry. The third section of this chapter will utilise the same analysis used in the first section on the case study of the cyber-attack on Norwegian oil and gas companies. Specific focus will be placed on Statoil and their management of the cyber-attack in comparison to Saudi Aramco's management. The last section of this chapter will look at how oil and gas companies can either manage or mitigate the risk of these identified vulnerabilities to cyber-threats. This final section will also establish and show just how complex and difficult it is and will be for oil and gas companies to develop plans and strategies to manage and mitigate the risk of cyber-threats.

### **4.2 Cyber Attack on Oil and Gas Companies in Saudi Arabia**

One of the most publicised cyber-attacks on an oil and gas company is the one on Saudi Arabian Oil Company (more commonly known as Saudi Aramco), which is a state-owned Oil Company located in Saudi Arabia. Saudi Aramco is a producer, manufacturer, marketer and refiner of crude oil, natural gas and petroleum products (Bronk & Tikk-Ringas, 2013:3). Saudi Aramco is considered to be the leading player in the petroleum industry as well as being the world's most valuable company (Perloth, 2012). Historically, the earnings made by Saudi Aramco have not been publicised but in 2019 they opened their books for the first time. In opening their books, it revealed that Saudi Aramco had generated a net income US\$111.1 billion in 2018 which makes it the most profitable company in the world by far (Reed, 2019). Saudi Aramco's net income outstrips competitors such as Royal Dutch Shell (US\$23.9 billion) and Exxon Mobil (US\$ 20.8 billion) (Reed, 2019). While this does reveal how highly profitable Saudi Aramco is, it also acts to show that this profitability is tightly bound to one country.

Saudi Aramco is headquartered in Dhahran, Saudi Arabia and they manage the world's largest proven conventional crude oil and condensate reserves of 259.7 billion barrels and ranks among the world's top refineries and natural gas liquids' exporters. Established in 1933 and owned entirely by the Government of Saudi Arabia since 1980, this corporation represents a bundle of strategic business interests (Bronks & Tikk-Ringas, 2013:3). It is important to note that Saudi Arabia is an absolute monarchy, as a result the government is dominated by the royal family. The conglomerate still holds subsidiaries and affiliates in the United States, the Netherlands, United Kingdom, China, Japan and Singapore.

#### **4.2.1 Events Prior to Shamoan Attack**

Prior to the Shamoan attack on Saudi Arabia there were two cyber-attacks that acted as precursors to the Shamoan cyber-attack on Saudi Aramco. The first of these cyber-attacks, titled the Stuxnet cyber-attack, occurred in 2010. The second cyber-attack titled Flame occurred in 2012, a few months prior to the Shamoan attack. Both of these attacks targeted Iran's oil and gas industry. Both should have acted as warnings to Saudi Aramco of their potential vulnerability to the risk of cyber-threats. In addition, both cyber-attacks had aspects that would have had the capability of gaining control of the

operational systems of Saudi Aramco. Stuxnet was first discovered following reports that there was a new computer malware that was spreading rapidly across the Internet in 2010 (Bronk & Tikk-Ringas, 2013:82). While both these cases may appear to be separated from the Shamoon attack they are not. Each of these attacks, as already stated, should have acted as warnings to Saudi Aramco and the oil and gas industry as a whole.

While Stuxnet was only discovered in 2010 it is believed by some that it had been in development since 2005. Iran was considered to be the main target of the Stuxnet cyber-attack. The attack resulted in there being significant disruption and damaged caused to Iran's uranium-enrichment through dramatically altering the speed of centrifuges at Iran's facility at Natanz (Bronk & Tikk-Ringas, 2013:82). When Stuxnet was discovered, it was reported that there was a concentration of the virus found in .id (Indonesia), .in (India) and .ir (Iran) domains (Johnson, 2016:92). Those who have studied the Stuxnet malware have considered it to be a very sophisticated worm (Bronk & Tikk-Ringas, 2013:82). It is important to note that even now it is still unknown how Stuxnet was introduced but it was specifically designed to target unknown zero-day vulnerabilities, which exist in Windows operation systems and elevate permissions. The zero-day exploits allowed for a complete system compromise by outside users. For years prior to the attack, they went completely undetected by both cyber-security researchers and larger software development communities. A reason why Stuxnet may have gone undetected, was that it was made to appear as if it were a valid device driver software that had come from a reputable developer (Bronk, 2016:83). The fact that the Stuxnet malware was capable of appearing as a valid device driver software also acts as an indicator of the sophistication of the attack.

Another reason Stuxnet is considered to be sophisticated is the payload it was carrying. Typically, a computer worm is used for other means such as Denial of Service (DDoS) attack or sending spam e-mails but the Stuxnet worm did not do this. Instead Stuxnet worm was designed with specific instructions for it to target systems Siemens Simatic Series 7 programmable logic controller (PLC) computers, which are the brains behind the operation of SCADA systems (Bronk, 2016:83; Johnson, 2016:92). The Stuxnet worm was capable of controlling and monitoring the systems it had infected while continuing to keep its presence hidden. PLCs in SCADA systems are used

throughout the oil and gas industry and oversee numerous operations. While PLCs are useful in running machines, they are only capable of doing so within very specific parameters with very little tolerance for variation or fault. Stuxnet's ability to take control on PLCs and rewrite instructions is very concerning for oil and gas companies as PLCs are used in a majority of oil and gas companies all across the world.

The second cyber-attack that Saudi Aramco should have taken as a warning was the Flame virus. The virus, which is a form of Spyware worm, is believed to have been jointly developed by the US National Security Agency, the CIA and Israel's military (Nakashima, Miller & Tate, 2012). It is believed that this joint venture started as far back as 2007. However, following the attack and upon further investigation all parties denied all and any involvement. Reports covering the Flame virus started to surface in May 2012 due to Iran detecting a series of cyber-attacks on its oil industry as well as other computers across the country that had been infected by a rather sophisticated computer virus (Nakashima, 2012; Nakashima, Miller & Tate, 2012). It is believed by some experts that Flame utilised the data, which had been exploited by Stuxnet, to launch their attack however, this is just conjecture (Johnson, 2016:93). Researchers did find that the Flame malware did identify more zero-day exploits in Microsoft Windows system. This acts to explain why researchers also found that Flame mainly attacked computers, which were running Microsoft Windows OS as well as the malware being utilised to conduct cyber-espionage against various countries.

Flame, much like Stuxnet, was utilised to target very specific systems or network components. Flame's ability to target these different systems and networks was aided by the fact that it was capable of evading the majority of security software. The Flame malware was capable of doing this as it adopted a Rootkit approach which essentially means that it attacked the Microsoft Windows OS at its root thus allowing the malware to bypass security systems (Johnson, 2016:93). This points to the sophistication of the Flame virus. Another similarity to Stuxnet, reported by security companies CrySIS Lab and Kaspersky Lab, is that Flame had been operating on the operating system for four years already (Perloth, 2012: Johnson, 2016:93). This discovery is concerning as they can only guess what data and information could have been collected by the malware in the years it operated undetected.

The Flame malware contained an erasing mechanism that was given the name wiper. The wiper mechanism is most probably the most concerning aspects of the Flame cyber-attack as it was the factor which most impacted the oil and gas industry in Iran. According to Iranian oil ministry officials, it was this wiper software code that forced them to shut off their Internet connection to their oilrigs and the Kharg oil terminal (Perlroth, 2012). Breaking the Internet connection between the Kharg oil terminal is concerning as the terminal is responsible for eighty percent of Iran's oil exports. The most concerning aspect about these findings is this same wiper software code, as will be discussed later, is the exact same component found within the code of the Shamoon cyber-attack. The directors and managers at Saudi Aramco should have analysed the findings of the reports and started to implement mitigation and management strategies, especially in light of its proximity to Iran and the fact that they are Saudi Arabia's primary regional rival (Dehlawi & Abokhodair, 2013). Another aspect of concern for Saudi Arabia is the ties to the US, which has already been the target of terrorist attacks. Saudi Aramco would be an ideal target for Iran to exact revenge for the Flame cyber-attack considering the belief that the US was a partner in the attack.

#### **4.2.2 Saudi Aramco's Cyber-security prior to Shamoon attack**

Before looking at Saudi Aramco's cyber-security prior to the Shamoon attack it is important to look at their approach to physical security. Former Executive Director of Saudi Aramco affairs, Abdullatif Othman, established the importance placed on ensuring the safety of their facilities when he stated that for years they have recognised how important it is to protect their vital facilities (Cordesman & Obaid, 2005:320). Even prior to Saudi Aramco experiencing any form of terrorist attacks, the company maintained a very high level of security. Saudi Aramco later placed even more importance on the physical security of their infrastructure following a thwarted terrorist attack on one of their massive petroleum-processing complexes at Abqaiq. Following the attack on Abqaiq, Saudi Aramco began consulting and working with experts and companies from the US to help create contingency plans as well as security solutions (Bronk & Tikk-Ringas, 2013:6).

Saudi Aramco's physical security was so well established that in 2010 they were acknowledged by the American Society of Industrial Security for their efforts. Saudi Aramco has placed such high importance on protecting their physical infrastructure from terrorist attacks as they recognised even a partial disruption to their facilities, in any area, would result in there being an immediate influence on oil and gas prices along with the knock-on effect for the global economy. Yet, despite Saudi Aramco's high concern for physical security they did not factor in the rising threats of cyber-attacks to their physical infrastructure. Very little is known about Saudi Aramco's cyber-security capabilities which is interesting considering their coordination with US experts as cyber-security started becoming a concern following the 9/11 terrorist attacks on the US as was outlined in Chapter 2. However, this may be on purpose as it would be counterintuitive for the company to publicise how they dealt with threats. This unwillingness to share is ultimately one of the biggest issues when it comes to addressing cyber-threats in the oil and gas industry.

As a result of the fact that there is very little known about Saudi Aramco's cyber-security, there is a limited amount of literature available to the public in either English or Arabic, with the exception of a few media mentions (Dehlwai & Abokhodair, 2013). One key source in particular is an article, which was written by Prince Naef Bin Ahmed Al-Saud, who is Brigadier General and a member of the Saudi royal family. The article was entitled *A Saudi Outlook for Cyber security Strategies Extrapolated from Western Experience* and was published in the first quarter of 2012. As result, it could have provided an idea of what cyber-security policy or initiatives would have been in place prior to the Shamoon attack on Saudi Aramco. The article primarily focuses on what steps the US has taken in forming and creating cyber-security policies. Special focus was placed on the partnerships between the US Department of Defense and different industries. Yet, in the article Al-Saud failed to actually provide any details with regard to cyber-security in the kingdom at all.

While he did not provide any details, Al-Saud did imply that at the time of the article was written no financial incentives were being provided for companies in Saudi Arabia to invest in cyber-security. Another issue was that there was no coordination between the Ministry of Defence and other critical infrastructure stakeholders, such as the board

of directors of Saudi Aramco, regarding cyber-defence. Ironically, Al-Saud provided a hypothetical scenario using Saudi Aramco as his example of how a cyber-attack could be a serious concern to Saudi Arabia (Al-Saud, 2012:78). Al-Saud believed that if hackers were to compromise Aramco computer systems it could possibly be considered a national security threat to Saudi Arabia. Following the Shamoon attack Al-Saud's hypothetical scenario was proven to be true as the Interior Ministry stated the following: "the August cyber-attack on Aramco's computer network targeted not just the company but the Kingdom's economy as a whole" (Dehlawi & Abokhodiar, 2013). Al-Saud does provide insight into how little attention had been given to cyber-security in Saudi Arabia, but it fails to answer critical questions on any actual existing cyber-security policies or the future of cyber-security policies in Saudi Arabia.

#### **4.2.3 Outline of the events of the Shamoon attack on Saudi Aramco**

On 15 August 2012 at 11:08am (Saudi-Arabian time), Saudi Aramco was the target of the cyber-attack Shamoon, also referred to as W32.Dsttrack. According to numerous reports on the Shamoon attack, it is considered to be the most destructive and the worst hack to ever been seen (Pagliery, 2015; Perlroth, 2012). Shamoon is a self-replicating computer virus initiated by an unknown person with the virus overwriting files on the hard drives of roughly thirty thousand of windows-based computers. Shamoon effectively erased three quarters of Saudi Aramco's data including documents, spreadsheets, e-mails and other files. All of the files that were erased by the Shamoon malware were replaced with an image of a burning American flag. The date of the cyber-attack plays a significant role in the cyber-attack as the evening of 15 August is Lailat al Qadr, which is one of the holiest days of Ramadan (Perlroth, 2012; Bronk, 2016:88). As result, over 55,000 Saudi Aramco employees had stayed home that day in order to prepare for the occasion, which meant there were not enough people to be aware of the problem or respond quickly to it either.

This left Saudi Aramco computer technicians, who were available, frantically ripping cables out of computer servers at data centres all over the world. By physically unplugging the computers from the Internet the technicians hoped to prevent the virus from spreading any further (Pagliery, 2015). Along with physically unplugging computers, Aramco took further measures to prevent Shamoon spreading any further



such as shutting down their corporate internal network, disabling all Aramco employees' e-mails and cutting off Internet access. Saudi Aramco immediately announced to the wider public that they had taken these measures but made no further comment on the attack. The Shamoon attack was kept from being far more devastating as Saudi Aramco had separated oil production from the company's internal network. This deliberate separation of the company's network from their production facilities could be a possible mitigation or management strategy the company put in place in order to protect their infrastructure from cyber-threats.

A group of hackers who called themselves the Cutting Sword of Justice took responsibility for the attack on Saudi Aramco a few hours after the cyber-attack had begun. The group posted the following message on PostBin, which is a hacker forum, a few hours after the attack had begun which stated the following:

We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighbouring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action. One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people. In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours. This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.  
(Untitled, 2012).

Their message provides an understanding that while Saudi Aramco was the target of the cyber-attack it was also mainly a means to an end. The main target was the Al



Saud royal family, for as the group states in their reasoning they perceive the Al Saud regime as being corrupt and continuing to support so called tyrant countries through the use of Muslim oil. The group targeted Saudi Aramco as it is the largest financial provider to the Al Saud regime and thus one of the most effective methods of targeting the regime. While a cyber-attack on Saudi Aramco would have an effect on the Al Saud regime there is the possible advantage of disturbing other Western economies through the same attack. Thus, providing those responsible for the Shamoon with a political motivation for their attack on Saudi Aramco. Ultimately, this message does provide a motivation for why the cyber-attack occurred and why Saudi Aramco was attacked and who was behind the attack. However, this became a more complicated issue once a deeper more thorough investigation began on the Shamoon attack, which will be discussed further in the next section.

Only after Saudi Aramco had established that oil exploration and production had not been affected did the president and CEO Khalid Al-Falih make an official statement on the company's Facebook page. Al-Falih firstly assured the wider public that their workstations had been cleansed of the virus, which they had done through replacing tens of thousands of the company's computers' hard drives (Perlroth, 2012). Al-Falih continued his statement with the following:

[Saudi Aramco] addressed the threat immediately, and [our] precautionary procedures helped to mitigate these deplorable cyber-threats from spiralling. Saudi Aramco is not the only company that became a target for such attempts, this was not the first nor will it be the last illegal attempt to intrude into our systems, and [Saudi Aramco] will ensure that [we] will further reinforce [our] systems with all available means to protect against a recurrence of this type of cyber-attack. [Saudi Aramco] would like to emphasize and assure [our] stakeholders, customers and partners that [their] core businesses of oil and gas exploration, production and distribution from the wellhead to the distribution network.

(Bronk & Tikk-Ringas, 2013:86; Fineren & Bakr, 2012).

In Al-Falih's statement confirms the fact that the separation of their internal network from their oil production was a deliberate mitigation strategy to protect the company from cyber-threats. The statement, also, mentions that Saudi Aramco was not the

only target of this attack. This could be alluding to the fact that Saudi Aramco was not the only oil and gas company hit by the Shamoon virus. Copies of the Shamoon virus were found on the computers of RasGas, based in Doha, Qatar, which is a joint venture between the nation of Qatar and ExxonMobil (Bronk, 2016:88; Zetter, 2012). Al-Falih's statement also draws attention to the fact the Saudi Aramco recognised that they would need to continue to improve their mitigation strategies of cyber-threats in order not to be subjected to such an event again. Following this announcement, a much more detailed investigation of the Shamoon attack began.

#### **4.2.4 Further investigation of the Shamoon attack on Saudi Aramco**

Shortly after Al-Falih's statement was posted on Facebook stating that the company was back online and operating, Saudi Aramco's website remained inaccessible to the public. In addition, Reuters sent e-mails to people within Saudi Aramco only to have them continually bounce back (Fineren & Bakr, 2012). Two months later these problems continued to occur with employees being unable to access their corporate e-mail and the internal network. Saudi Aramco's executives, following the Shamoon attack recognised that their systems were still vulnerable. In order to manage the vulnerability to cyber-threats executives stopped their employees from being able to gain access to Saudi Aramco's internal network remotely. It actually took Saudi Aramco roughly five months to fully come back online (Rashid, 2015). In Chapter three, it was discussed that in the upstream sector a lot of value is placed on both drilling and production data that is a vulnerable sector for cyber-attacks. The Shamoon attack acts to highlight this very vulnerability as it wiped Saudi Aramco's data from their hard drives. Saudi Aramco lost both its production and drilling data, which included drilling data from companies such as Santa Fe, Ocean and Schlumberger (Roberts, 2012). Saudi Aramco held all the filtered data stored on their systems, which typically would be stored and backed up twice a day. However, due to employees being out for Lailat Al Qadr no back-ups of the filtered data were saved that day (the filtered data holds the most value not the raw data). The loss of this data was something Saudi Aramco did not address in their statement despite the fact that they had actually lost valuable information for the company belonging to the company.

As different companies started examining and analysing the malware and its main components, they started to identify the key components of the malware as well as errors in coding of the malware.<sup>17</sup> Symantec, a software company offering cyber-security software and services, identified that Shamoon actually launched a three-pronged attack. Symantec were able to breakdown the components of the malware into these three parts: a Dropper, a Reporter and a Wiper (Johnson, 2016:95; Bronk & Tikk-Ringas, 2013:85; Perlroth, 2012). The Dropper module is the main component of the malware as it is the original source of the malware and then supports the spread of the malware across the infected network of machines. The Reporter module is responsible for collecting the data from the computers infected and sending it back to the source of the malware. The Wiper module is the most destructive part of the malware as it is responsible for destroying all the data on the infected computer and replacing it with the image of the burning American flag and in the process removing the evidence of the malware from the computers to cover any traces of the attack. The identification of the wiper module started to raise questions about whether or not the Cutting Sword of Justice were actually the ones responsible for the Shamoon cyber-attack on Saudi Aramco.

As was previously discussed in the first few days following the Shamoon attack, before the malware was examined, the belief remained that the Cutting Sword of Justice was responsible. However, once more in-depth investigations were begun by various security groups and government departments, the validity of the Cutting Sword of Justice actually being responsible for the attack on Saudi Aramco started to be questioned. Focus immediately turned to Iran being the ones actually responsible for Shamoon. Iran became the focus due to the identification of the Wiper module in malware as it had the same main component of the Flame cyber-attack against them. Some investigators believed that Iran was merely using the Cutting Sword of Justice as a front to hide behind but this was merely inferential reasoning which could have led investigators astray. However, Iran did have a

---

<sup>17</sup> The error in coding was identified by Kaspersky which they spoke about in their report on Shamoon. However, going into further detail on coding issues falls outside the scope of this study.

motive to have launched the cyber-attack against Saudi Aramco as economically they were suffering under tightening sanctions in 2012.<sup>18</sup>

These tightening sanctions heavily impacted the Iranian oil and gas industry and resulted in a lot of their oil going unsold while Saudi Arabia continued to produce ten million barrels per day. The sanctions also made it difficult and expensive for Iran to resume their stalled oil production. Saudi Arabia is Iran's regional competitor and Saudi Arabia were not responsible for any of the sanctions against Iran. However, Iran could have decided to use Saudi Aramco as a target of a cyber-attack due to their relationship with the US and as they export a large amount of their oil to the US. Thus, through targeting them the US would essentially also be affected economically and politically because of their economic reliance on the import of oil. This thinking about Shamoon should act as reminder to key infrastructures, such as Saudi Aramco, that they need to be alert to the fact that they could become political or economic targets of cyber-threats. The development of these perceived motivations, in addition to the identification of the Wiper module, resulted in US intelligence officials strongly refuting the notion of the Cutting Sword of Justice being responsible and stated only Iran would actually have the cyber-ability to mount an attack like Shamoon. Despite making these claims, US intelligence never provided any information or evidence to support this claim. Therefore, their claim is merely speculation (Perlroth, 2012). Despite US intelligence and other investigators pointing to Iran as being responsible, Iran officially and publicly denied having any part in the construction and deployment of Shamoon (Bronk & Tikk-Ringas, 2013:24). While there is evidence to support Iran being responsible, they were not the only source considered to be behind the Shamoon attack on Saudi Aramco.

Some investigators have stated that the Shamoon attack had to have involved an insider. Investigators state that only an employee or contractor of Saudi Aramco

---

<sup>18</sup> In 2012 the US imposed sanctions against Iran's central bank which is the clearing house for Iran's oil export profits. Additionally, the European Union (EU) put in place an oil embargo in order to get Iran to stop their nuclear programme. US put forward a second sanction, which banned any of the world's banks from being able to complete oil transactions with Iran. The EU also put in a second sanction, which officially banned Iranian oil exports (Timeline: Sanctions on Iran, 2012).

would have had the ability to introduce the Shamoon malware on their internal network. This could have been done through unknowingly opening a link in an e-mail infected with the malware or by purposely copying it from a USB device (Perloth, 2012; Bronk & Tikk-Ringas, 2013:18). While Saudi Aramco found possible individuals who could have been behind the attack, the names were never disclosed due to the company not wanting to comment on an on-going investigation. Ultimately, finding that someone inside the company played a role in the Shamoon attack raised important questions for Saudi Aramco in regards to how they implement their cyber and physical security measures. The greatest issue with different investigators and institutions pointing fingers as to who is responsible indicates how incredibly difficult it is to identify those actually responsible for cyber-attacks like Shamoon. The finger pointing also only makes the process of identifying those behind a cyber-attack even more difficult because of the lack of consensus.

Three years after the Shamoon cyber-attack on Saudi Aramco, Chris Kubecka, spoke about her experience during the events of the Shamoon attack. Kubecka, a former security advisor to the company, had been hired by the company following the attack in order to make sure that Saudi Aramco's satellite offices in Africa, Europe and the Middle East remained secure (Rashid, 2015; Pagliery, 2015). Kubecka stated that while the company's drilling and exploration production had not been interrupted, the same could not be said for the rest of the business as it was in turmoil. As result of the company being forced to go offline as a protection against further damage, things such as managing supplies, shipping, contracts with governments and business partners were all required to happen on paper (Pagliery, 2015). Another issue caused by the shutdown, according to Kubecka, is that all the company's payment systems were affected too, which resulted in miles of domestic gasoline tank trucks being turned away as they could not be paid. This continued for seventeen days following the attack until the company eventually started to give the oil away for free to ensure that it kept flowing within Saudi Arabia. Kubecka also drew attention to the fact that the oil and gas industry was not the only industry influenced by the Shamoon attack on Saudi Arabia.

As discussed in the previous section, Saudi Aramco bought hard drives to replace the ones infected on all the company's computers. Saudi Aramco did this by flying representatives of the company directly to computer factories in Southeast Asia, where they bought every single computer hard drive in the manufacturing line. Saudi Aramco was capable of doing this because of their high revenue which gives them the advantage of being able to buy the hard drives and replace them quickly. Saudi Aramco bought roughly fifty thousand hard drives at a higher price than every computer company in the world in order to get the hard drives (Pagliery, 2015). At the time, the world supply of hard drives was already under pressure due to flooding in Thailand. Saudi Aramco purchasing the hard drives brought the supply to a halt. In addition, the prices for hard drives increased which increased the price of computers from September 2012 to January 2013.

It is important to note that buying the hard drives was merely the fastest method to enable Saudi Aramco systems to get up and running without the virus. The original drives could have been reused and rebuilt after they had been wiped. In doing this Saudi Aramco could have tried to recover some of the lost data but it would have been far too time consuming. This is interesting as it shows that while the company had maintained oil production and exploration the crippling of the internal network had its own devastating effects. This acts to demonstrate that despite Shamoon not being considered sophisticated, by companies such as Kaspersky, it did not have to be to inflict the amount of damage that it did. While Saudi Aramco might have only been knocked down by Shamoon temporarily, it took a significant amount of time for the company to fully recover from the attack. If any other company had been targeted, they would not have had the same outcome, especially a smaller company, which would not have had the same resources available to them as Saudi Aramco does.

#### **4.2.5 Legacy of Shamoon Attack on Saudi Aramco**

While Shamoon did not result in impacting Saudi Aramco's oil production and exploration infrastructure it did have a financial impact on the company and the operational side of the company. Saudi Aramco's experience with the Shamoon cyber-attack forced a much larger change by making oil and gas companies worldwide alter

the way they approach the risk assessments of their key infrastructures. In particular, it has forced companies to pay attention to the risk cyber-threats pose as they are no longer a far-fetched notion, Shamoon shows just how real the threat of cyber-attacks is.

Saudi Aramco managed to remove the Shamoon malware from their corporate computers through replacing all of the company computer hard-drives but it did not actually destroy the malware itself. As a result, in 2016/2017 different companies in Saudi Arabia were hit by an updated version of Shamoon. One of the targets of particular interest is Sadara Chemical Company (Perlroth & Krauss, 2018). Sadara is of interest as it is a joint venture between Dow Chemical and Saudi Aramco, which means this was the second time that Saudi Aramco had been attacked by Shamoon, even if they were hit indirectly. Much like Saudi Aramco, the Shamoon 2.0 virus again exploited a zero-day exploit in the Microsoft operating systems and forced Sadara to shut down their computer network while they dealt with the attack. They stated that operations at the facility were not affected by the down time. It appears that Sadara were able to recover faster than Saudi Aramco, which suggests that Saudi Aramco's experience with Shamoon meant they knew how to help Sadara recover quickly. Ultimately, this second Shamoon cyber-attack demonstrates another challenge of cyber-threats which is that while oil and gas companies can recover from cyber-attacks they will never actually be rid of future threats of suffering from the same malware or an updated version of it in the future.

#### **4.2.6 Second Cyber-attack on a Saudi Aramco Petrochemical plant**

In mid-March, 2018 the first reports of yet another cyber-attack started to emerge. The cyber-attack, called Triton, had been carried out against a Saudi Arabian petrochemical plant. The attack occurred eight months prior to the attack being reported because the investigators remained tight-lipped about the cyber-attack. The investigators being tight-lipped emphasises the issue of the lack of information sharing about cyber-attacks between oil and gas companies. Oil and gas companies need to share information in order to properly start developing mitigation and management strategies that are effective. The attack was a different kind of cyber-attack, unlike any they had experienced before as unlike Shamoon this cyber-attack was not designed with the intention of shutting-down systems or stealing data, it had a far deadlier goal. The

cyber-attack was meant to sabotage the plants industrial control systems and cause an explosion (Perlroth & Krauss, 2018). The only reason why the malware failed in achieving its goal was that there was a minor error in the coding of the malware.

Investigators are unwilling to disclose the company which was the target of the attack while Area 1 Security, a computer security firm founded by veterans of the US National Security Agency, stated in a confidential report that they had identified Saudi Aramco as the petrochemical plant which was attacked (Groll, 2017). Others who have investigated the attack have agreed with the findings of Saudi Aramco being the target of the attack, while others are unwilling to support these findings due to Saudi Aramco's denial of being the target. This denial could be due to their unwillingness to damage their public reputation, as Saudi Aramco was in the process of preparing for the largest public offering of all time. The company's IPO (initial public offering) has been staked as a sweeping reform plan, which sought to diversify Saudi Arabia's economy by Saudi Crown Prince Mohammed bin Salman (Groll, 2017). Saudi Aramco being the target of a second known cyber-attack in four years would clearly have a negative influence on the up-coming public offering of the company which would impact attempts to diversify the economy outside of oil and gas. Furthermore, no one who was investigating this second Shamoon attack was able to identify who could have been responsible or behind it.

The Triton cyber-attack acts as a marker to indicate how cyber-threats and attacks are escalating and how hackers are displaying both the drive and the ability to cause some serious physical damage to critical infrastructure and employees (Perlroth & Krauss, 2018). The American-engineered computer systems, which were compromised in the Triton attack, are utilised by oil and gas companies all over the world. This has caused concern for US government officials, as well as their allies and cyber-security researchers, that a cyber-attack such as this could be replicated and used against another oil and gas company. Investigators found that a computer in the engineering workstation had a peculiar file on it that looked like it should be there, but this file held the malware that sabotaged the systems. Investigators said that the file had not been put there by an inside man; this points to the malware sabotaging the system remotely (Perlroth & Krauss, 2018). Another cause of concern was that while an error in the



malware's code stopped it from achieving its deadly goal, investigators truly believe that the hackers could have fixed this coding error. The implication is, that it is only a matter of time before the updated Triton malware is deployed against another industrial control system. The updated Triton malware components can easily be sold to others seeking to cause damage or harm to other industrial control systems on websites such as eBay.

A greater point of concern with the Triton cyber-attack was how sophisticated the attackers had been in the coding of the malware. Those responsible for the attack had to have understood the design of the control system as well as the layout of the petrochemical plant as they needed to know which pipelines went where and which valve did what in order to know which one to turn-off to cause an explosion (Perlroth & Krauss, 2018). This sophistication indicates to investigators that the individuals behind the attack took their time developing the malware and had plenty of resources available to them. Still investigators were unable to identify there being any sort of profit motivation in the Triton attack. This is concerning as it indicates that those behind the development of the malware were most likely being supported by a nation-state. According to cyber-security experts very few nation-states possess this level of technical sophistication which quickly narrowed down the list of nation-states to Iran, China, Russia, the US and Israel.

Despite these five nation-states having the technical sophistication to carry out an attack such as Triton, according to the initial investigation none of them appeared to have the motivation to carry out this attack except for Iran. Investigators ruled China and Russia out as both nation-states had in the previous years been making increasingly more energy deals with Saudi Arabia. Israel and the US were ruled out as an option as both states were working in cooperation with Saudi Arabia in dealing with Iran. This left Iran as the only viable option seeing as tension between Iran and Saudi Arabia had only increased over the years prior to this. Additionally, Iran has started growing their military hacking programme. While they might be the only viable option as being the nation-state behind the attackers, Iran denied having been involved with the Triton malware. These initial findings would be brought into question with the publication of a more in-depth report covering the Triton malware.

During October 2018 FireEye, a major cyber-security company, published their report concerning the Triton cyber-attack. FireEye identified that the Scientific Research Institute of Chemistry and Mechanics, located in Moscow, was behind much of the effort of the creation of the Malware. The Institute has deep ties with the Russian government, which date back to before the 1917 Bolshevik revolution (Sanger, 2018). The involvement of the Institute raises many unanswered questions about why Moscow would even target a Saudi Arabian plant. One possible reason is that Russia and Saudi Arabia are rivals in the petroleum marketplace, but this does not seem to be enough motivation. This has brought about speculation that Iran was still actually behind the attack but that they had had a lot of help from Russia. When developing the malware Iran could possibly have sent the malware to the Institute to provide their expertise to help fine tune it. Another important discovery in FireEye's report is that even though much of the coding and activity to maintain and rewrite elements of the malware can be traced back to the Russian Institute, they did not initiate the attack. The Russian government has denied having anything to do with the placing of the malware.

In the greater scheme of things, this particular attack has garnered much more attention from experts concerning the issue of cyber-threats and the influence they have on the oil and gas industry due to their vulnerability. Following this attack more articles and reports started being published covering the evolving cyber-threat landscape in the oil and gas industry along with some suggestions on how these threats can be managed and mitigated. Despite the greater focus, the field still remains fairly limited on resources and information. For oil and gas operators in the Middle East greater pressure was placed on them, following the Triton attack, to do more to defend themselves against cyber-threats. The Triton attack also indicated that despite Saudi Aramco having experience with cyber-attacks and improved cyber-threat management strategies, there were still vulnerabilities in their system, which could be exploited.

At the beginning of 2019 it was announced that Saudi Aramco and Raytheon, a US-based security contractor, had partnered in a joint venture seeking to “develop, market and provide cyber-security services in the Saudi Kingdom and in the region” (Middle East oil and gas is prime target for cyber-attack, 2019). The announcement was made

just a few days after Italian oil and gas contractor Saipem had announced that hundreds of their servers in Saudi Arabia, as well as in United Arab Emirates and Kuwait, had been the target of a cyber-attack. A few days later, Pertrofac, a second oil field in the Middle East was attacked. Both companies work extensively with Saudi Aramco, which seems to indicate that due to Saudi Aramco being one of the top targets of cyber-attacks that by extension those closely associated with them can be targets as well.

#### **4.2.7 Evaluating the Presence of Vulnerabilities to Cyber-threats in the Saudi Aramco Case Study**

In Chapter Three, vulnerabilities to cyber-threats were identified and summarised in a table. It is important to draw a correlation between the vulnerabilities to cyber-threats in Chapter Three and whether or not they are present in the Saudi Aramco case study as well as those, that were not present. The following is an independent analysis of the case study and the vulnerabilities present. The first vulnerability to cyber-threats identified in the Saudi Aramco case is the lack of information sharing. Following the Stuxnet and Flame cyber-attacks on facilities located in Iran no information regarding the attacks was made public. This lack of information sharing led to Saudi Aramco being unaware of just how real the threat of cyber-attacks were in the region. However, it is important to remember that Iran would most likely not have been willing to share information with Saudi Arabia, especially not an oil and gas company such as Saudi Aramco. This is due to the fact that Saudi Arabia and Iran are regional rivals but this rivalry ties into another vulnerability identified in the Saudi Aramco case and will be discussed later in this section. While Saudi Aramco was made vulnerable to cyber-threats due to a lack of information sharing, they are guilty of the same thing. Following the events of both the Shamoon and Triton cyber-attacks, Saudi Aramco was unwilling to share information regarding their experience handling a cyber-attack within oil and gas companies.

The second most evident identified vulnerability found in the Shamoon attack was Saudi Aramco's overall low cyber-maturity. Saudi Aramco's low level of cyber-maturity is evident prior to the Shamoon cyber-attack as the company had no manage or mitigation strategy in place to deal with cyber-threats. Saudi Aramco's security plans solely focused on protecting their infrastructure from physical threats and thus did not

view cyber-attacks as a credible risk. This lack of cyber-maturity can be questioned, as the company had separated their corporate infrastructure from their operational infrastructure, which did prevent the Shamoon attack from being more deadly. Another vulnerability to cyber-threats is evident when studying Saudi Aramco's reliance on traditional methods of security, which could be seen in their utilisation of traditional anti-virus security software. The utilisation of traditional anti-virus security software, which is unable to detect the presence of malicious malware, allows malware to go undetected for extended periods of time. The reliance on traditional anti-virus security software leads to yet another vulnerability to cyber-threats found in the Saudi Aramco case, which is a lack of monitoring for cyber-threats. The lack of monitoring for cyber-threats in both the Shamoon and Triton cyber-attacks on Saudi Aramco they were vulnerable to cyber-attacks and caught by surprise.

Uneducated employees are another vulnerability present in the Shamoon cyber-attack on Saudi Aramco. When the Shamoon malware began to spread throughout the corporate computers, technicians did not know what to do to slow the spreading of the malware. Instead the technicians did the only thing they could think of which was to unplug all the computers. While this did stop the malware from further affecting other computers, if employees had been better educated and had, had a procedure to follow when a cyber-attack occurred fewer computers might have been infected.

A final vulnerability to cyber-threats present in the Saudi Aramco case is reputational risk. Saudi Aramco is the largest source of revenue for the Saudi Arabian government, which makes them highly vulnerable to cyber-threats. Saudi Aramco could be targeted as a result of nation-states or terrorist groups seeking to destabilise the Saudi Arabian government. Saudi Aramco is also vulnerable to politically motivated attacks due to the political conflict between Saudi Arabia and Iran as well as their close ties to the US.

### **4.3 Cyber-Attack on Oil and Gas Companies in Norway**

Before looking at the cyber-attacks on oil and gas companies in Norway can begin it is important to make a few important distinctions. Firstly, the literature and articles, which cover this cyber-attack in both English and Norwegian, is limited. The information available within these articles in regard to the events is even more limited. The majority

of the articles merely provide the same information. Secondly, as was noted back in Chapter One the influence that the cyber-attack had on Statoil will be the focus of this section. While it will be seen that numerous oil and gas companies were targeted by the cyber-attack, it is believed that Statoil was the primary target of the attack. Examining Statoil's experience with a cyber-attack provides an interesting comparison in how an oil and gas company in a developed country and one in a developing country experience a cyber-attack. Additionally, Statoil is somewhat similar to Saudi Aramco in terms of the fact that the government owns a majority of the company's shares. Statoil is a vital contributor to Norway's economy and state revenues much like Saudi Aramco. However, the manner in which the cyber-attack on Statoil and the way in which they dealt with the cyber-attack are vastly different. Unlike the Shamoon attack on Saudi Aramco, Statoil has divulged very little information regarding their experience about the cyber-attack as the problem was dealt with internally without outside assistance.

#### **4.3.1 Statoil cyber-security prior to the 2014 cyber-attack on Norwegian oil and gas companies**

According to a Norwegian article, following the Shamoon attack on Saudi Aramco in 2012, Statoil started following the development of these new cyber-threats to the oil and gas industry (Helgesen, 2013). This points to one of the first differences between Saudi Aramco and Statoil's management of cyber-threats, as unlike Saudi Aramco who did not start following the events of cyber-threats prior to Shamoon, Statoil's management recognised the necessity of monitoring them. Additionally, according to Statoil's press spokesman, Ola Anders Skauby, the company used a considerable amount of resources to put in place technical and procedural barriers. Statoil has focused on raising the competence of the individuals who work with process control systems regarding information security. Another fact, which makes Statoil interesting as the target of a cyber-attack, is the findings published in an incident report at the end of 2013. January 2013, roughly six months after the Shamoon cyber-attack, a terrorist attack was carried out on the In Amenas facility in Libya, which was a joint venture between Statoil, BP and Sonatrach. The attack had been unexpected and had devastating consequences and as such Statoil conducted an independent investigation on the attack. The purpose of the investigation for Statoil was to determine the likelihood of a similar attack occurring in the future and how well established their

security was (Boman, 2015)<sup>19</sup>. One of the findings of the report was that Statoil lacked a security culture as well as a security system, which is inadequate for an international company.

The most important conclusion of the report was that the greatest long-term threat facing the company in the future is not actually physical attacks but rather cyber-attacks on the company. According to Adam Fulcher who is the Head of Security at Statoil, the fact that the majority of Statoil's assets are located in Norway created a relaxed culture towards security. Fulcher stated that if Statoil's industrial control systems were to suffer a major large-scale accident it would ultimately result in shaping and changing the future course of the company (Boman, 2015). Following the outcome of the report Statoil started to establish a security improvement programme, which would address different aspects of security. In regard to their cyber-security issues Statoil believes that security will need to be risk-based as well as intelligence-led.

The Norwegian government has allowed Statoil to have access to intelligence information in order to help the company address security issues. This does provide the company with an advantage in regard to having the necessary information available to them (Boman, 2015). However, establishing these close connections with the government can result in Statoil being the target of a cyber-attack in an effort to hurt the government, such as the Shamoon attack on Saudi Aramco. In examining their cyber-security Statoil also identified two key problems in preventing and mitigating cyber-attacks both of which would be challenges to any oil and gas company addressing cyber-threats. The first big challenge is that there is a lack of common standards which suppliers and vendors are held to when it comes to providing reassurance against cyber-threats. Thus, despite cyber-security measures being implemented by Statoil, these security measures will not be effective if vendors and suppliers of equipment and products are not being held to the same standard.

---

<sup>19</sup> Karen Boman's article *Fulcher: Cybersecurity Ranks as Top Long-Term Threat to Statoil*, will be heavily relied on throughout this section. This is due to the fact that she is one of the only people to write about the API Cybersecurity Conference in Houston in 2015 where Adrain Fulcher spoke about Statoil's security threat assessment following the In Amena's terrorist attack.

The second big challenge facing the management and prevention of cyber-attacks is that nation-states are becoming increasingly more reliant on cyber-attacks rather than physical methods to hurt the economy of other nation-states (Boman, 2015). Historically, Statoil has utilised the special military forces provided to them by the Norwegian government to protect their infrastructure from physical threats, but these will not be useful against cyber-attacks. Thus, now it is the responsibility of oil and gas companies, such as Statoil, to protect their infrastructure. Fulcher states that due to this change, oil and gas companies and host governments need to establish a comprehensive understanding of what responsibilities the oil and gas companies have for protecting their physical infrastructure and what protection would be provided by the foreign government which hosts the oil and gas company's facilities (Boman, 2015). Despite Statoil being aware of the fact that their greatest vulnerability is now cyber-threats, according to the findings of the incident report, they were still vulnerable to a cyber-attack.

#### **4.3.2 Outline of the Events of the Cyber-attack on Oil and Gas Companies in Norway**

In August 2014 over three hundred oil and gas companies in Norway were the targets of a cyber-attack. This cyber-attack is the largest cyber-attack to ever be coordinated in Norway. Prior to the attack occurring the Nasjonal Sikkerhetsmyndighet (NSM), which is the National Security Authority in Norway, had been forewarned about the attack by one of their international contacts (Bryne, 2014). NSM were then capable of issuing a warning to all the oil and gas companies, which they suspected could be targets of the pending cyber-attack. The hackers targeted the systems of the oil and gas companies by sending e-mails to key personnel within each company (Muller, Gjesvik & Friis, 2018:7). The hackers structured the e-mail to appear as if it had come from a legitimate source with an attachment to be opened. The attachment held the destructive malware designed by the attackers. If the person targeted opened the attachment the programme would be launched into the company's system.

Of the three hundred companies warned, it is estimated that roughly fifty oil and gas companies have already been breached while the remaining two hundred and fifty

remain at risk (Muller *et al.*,2018:6). Unlike with the Shamoon attack on Saudi Aramco little else is known about the cyber-attack and its influence. No group immediately took responsibility for the cyber-attack, like the Cutting Sword of Justice had done in the wake of the Shamoon attack. Even, following further investigation into the cyber-attack, which will be discussed further in the next section, speculation still remains as to who was responsible. Additionally, nothing is publicly known about how the fifty oil and gas companies breached by the cyber-attack addressed and dealt with their systems being attacked. This stems from the fact that few of these fifty companies breached even made any statement saying that they had been breached or even acknowledging the cyber-attack - one of which was Statoil. Statoil's statement both acknowledged and gave a minor insight into how they addressed the warning of the cyber-attack. The statement was given by Statoil's Head of Press, which went as follows: "we have received a warning and are checking on our systems according to routines" (300 oil and gas companies hacked in Norway, 2015). Statoil likely made the statement to assure public shareholders of the company that there was nothing they needed to worry about much like Saudi Aramco did following the Shamoon attack.

#### **4.3.3 Further Investigation and Findings of the Norwegian Cyber-attack**

Upon further investigation of the cyber-attack one of the concerning factors of this attack, according to Hans Christian Pretorius, Director of the Operative division of NSM, is that the hackers responsible had obviously done their research before they launched their attack (Munson, 2014). This research can be seen by the fact that the attackers responsible knew exactly which key functions to go after and who the key personnel of the different companies were (Munson, 2014). The complexity and how the cyber-attack specifically targeted key individuals indicates that the attackers were not mere novices; as well as them having large financial resources backing them. The fact that the attackers are believed to have received substantial financial backing points to the possibility of a nation-state being the ones responsible for the attack. However, no nation-state has been identified as having the necessary motive to support this attack. Pretorius continued in his statement that e-mails were the common denominator in the attack and the way to instigate the cyber-attack. Pretorius believes that, in general, Norwegians need to be more discerning or sceptical about e-mails sent to them, as they tend to be far too trusting and if they were more discerning it would help in combatting



cyber-threats (Hotvedt, Aardal, Lauritzen & Kristoffersen, 2014). In the case of this cyber-attack, if personnel opened the attachments it would have launched a destructive programme into the system of the company.

The destructive malware was designed to find vulnerabilities or holes in the security of the target companies' system. Once a vulnerability was identified a communication channel would open up with the hackers which would lead to the malware launching a much more serious attack on the company's system (Munson, 2014). It is believed by NSM that the primary objective of the cyber-attack was to install a key-logger that would steal passwords to get into one of the oil and gas companies' secure networks (Muller *et al.*, 2018:7). By accessing the secure network, the hackers could potentially steal confidential intellectual data from the oil and gas company. Unlike the Shamoon attack on Saudi Aramco no outside help was required to help the targeted companies address and deal with the outcome and recovery from the cyber-attack. While there is extremely limited information available covering any aspect of the cyber-attack on the Norwegian oil and gas industry, as previously mentioned one interesting finding was that Statoil was believed to be the primary target of the attack. However, before looking at Statoil it is important to look at further research conducted in regard to who was responsible for the cyber-attack.

While NSM may have warned oil and gas companies about the cyber-attack occurring, they originally stated that they did not know who was responsible or behind the attack. NSM, however, actually did have a slight indication of who could have been responsible for the attack but chose not to investigate any further as they stated it was not their responsibility to go after those responsible. Pretorius explains that NSM's responsibility is just to uncover data which points to threats of cyber-attacks and assist in helping oil and gas companies in handling them and in some cases preventing them (Hotvedt, Aardal, Lauritzen & Kristoffersen, 2014). As mentioned at the beginning of this section, Pretorius did indicate that NSM believed that the hackers responsible did not appear to be novices and had resources available to them that could have only been supplied by a nation-state. One potential hacker group has been identified that could potentially have been behind the attack: the Dragonfly group.

The Dragonfly hacker group (also known as the Energetic Bear) were first identified in 2011 by Symantec, following the group's successful cyber-attacks on thousands of companies around the world. Symantec believes that the Dragonfly group is following in the footsteps of the Stuxnet attack on the Iranian nuclear programme. The Dragonfly group first started with cyber-attacks that targeted defence and aviation companies in the US and Canada (Dragonfly: Western Energy Companies Under Sabotage Threat, 2014; Johansen & Færaas, 2014). In 2013, the group changed its target to the oil and gas industry in the US and Canada but later they widened their scope to Europe as well. This development led to Symantec reaching out to warn the oil and gas companies in Europe so that they would be aware of the threat the Dragonfly group posed to the industry. The attacks conducted by Dragonfly supports the notion that it is a state-sponsored operation due to the group displaying a high degree of technical capabilities. The nation-state sponsoring the group has yet to be identified but some point to Russia being responsible.

The Dragonfly group fits the theory put forward by NSM of the attackers being supported by a nation-state. Another reason why the Dragonfly group is believed to be behind the attack is because of the method that they used to infect systems. One of the earliest methods used by the Dragonfly group to infect a company's system with malware was through e-mail campaigns (Dragonfly: Western Energy Companies Under Sabotage Threat, 2014). Dragonfly's e-mail campaign consisted of identifying and targeting selected executives and senior employees of a company and sending them an e-mail. The e-mail would have one of two possible subject lines either "The account" or "Settlement of delivery problem" and would contain an infected PDF attachment (Dragonfly: Western Energy Companies Under Sabotage Threat, 2014). Dragonfly's e-mail campaign mimics the method used to gain access to the different Norwegian oil and gas companies' systems thus providing more motivation to support the idea that Dragonfly was responsible for the hack. Despite these findings supporting the notion of Dragonfly being responsible, NSM and other agencies remain unsure if they were actually responsible.

As previously stated, those investigating the cyber-attack on the Norwegian oil and gas companies believe that Statoil was the primary target of the cyber-attack

(Munson,2014; Muller *et al.*, 2018:6). The head of Statoil's press acknowledged the cyber-attack through making the following statement: "we have received a warning and are checking on our systems according to routines" (300 oil companies hacked in Norway, 2015). It is believed by some reporters covering the cyber-attack that Statoil was the primary target of the cyber-attack due to the role the company plays in Norway's economy. It is important to note that the petroleum sector plays a prominent role in Norway's national economy. In 2014, the Petroleum sector accounted for twenty percent of Norway's Gross Domestic Product (GDP), twenty-seven percent of the state's income and forty-six percent of all exports (Muller *et al.*, 2018:6). The Norwegian government owns a majority of Statoil's shares, sixty-seven percent, while the rest is public stock. As a result of the Norwegian government owning a majority of Statoil, the company is also one of the biggest contributors to the government financial resources.

This is similar to Saudi Aramco being the biggest source of income for Saudi Arabia, which is also owned by the Saudi government. Unlike Saudi Aramco, where the profits go to the Saudi royal family, the profits from Statoil do go towards the government's coffers and are utilised to support the so-called 'Scandinavian Miracle' (Leyden, 2014). While Saudi Aramco is considered to be a giant in the oil and gas industry, Statoil is far smaller, but it is the largest oil and gas company in Norway and is the largest energy supplier in Europe (Bryne, 2014). This, however, confirms one of the biggest challenges identified by Fulcher, which was that oil and gas companies would be targeted to harm a nation-state economically. It remains unknown who was behind the cyber-attack, which hinders further analysis into the motives of the attackers. Outside of Statoil acknowledging the warning and testing their system no other information has been made publicly available regarding what influence the cyber-attack had on Statoil. A possible reason for the lack of information from Statoil being made available about the cyber-attack is because the company keeps its cards very close to its chest. Statoil does not want to publicly share how many resources they use in order to protect against cyber-attacks or how many cyber-attacks they have detected (Becker, 2013). According to Statoil's IT director, they consider not sharing information as part of the risk picture because if they publicise how they deal with cyber-attacks it will inform hackers about how to work around their protections (Becker, 2013). As such, Statoil is continually

working towards new measures in order to regularly ensure their protection against any potential cyber-threats.

#### **4.3.4 Legacy of cyber-attack on Oil and Gas Companies in Norway**

While there may have not been any other information available covering the influence the cyber-attack had on Statoil it did leave a legacy. Unlike Saudi Aramco, its legacy was not a re-emergence of the cyber-attack and its malware but a legacy of increased focus on cyber-security. According to a report published by DNV GL, a classification society headquartered in Norway, there had been over fifty cyber-attacks on the oil and gas sector in 2014 alone (Janbu, 2016). Further research by DNV GL found that combatting cyber-threat challenges to security will become a very important area of focus for the oil and gas industry. In the case of Norway, DNV GL's research into cyber-threats has shown that only thirty-two percent of senior employees in Norway have any plan to invest in preventing, detecting and responding to cyber-threats (Janbu, 2016). These findings have reinforced the necessity of counter-measures that will be able to handle larger and more sophisticated cyber-attacks to oil and gas companies.

This awareness has seen DNV GL creating a joint project with Shell, Lundin, Siemens, Honeywell, ABB, Emerson, Kongsberg Maritime and lastly Statoil and will be observed by the Norway Petroleum Safety Authority. One of the main purposes of the joint project is for all of these companies to work together to develop and recommend methods of dealing with cyber-threats (Janbu, 2016). Through the different companies making recommendations the joint project hopes to create a guideline that can help protect oil and gas installations from cyber-threats and reduce cyber-attack incidents. There, however, is no one size fits all approach to securing oil and gas companies from cyber-threats. Additionally, the joint project seeks to cut the costs for operators, contractors and suppliers by reducing the resources that are needed to meet requirements. The overarching long-term goal of the whole joint project is to raise more awareness of cyber-threats to oil and gas companies and to educate staff.

#### **4.3.5 Evaluating the Presence of Vulnerabilities to Cyber-threats in the Norwegian Case Study**

Looking at the case of cyber-attacks, utilising the table of vulnerabilities to cyber-threats, a few of the identified vulnerabilities can be found in the Norwegian case study. The following is an independent analysis of the data presented from the case study of the cyber-attack on Norway. Unlike the Saudi Aramco, less vulnerability to cyber-threats can be found when looking at the events of the cyber-attack on Norwegian oil and gas companies. The identification of less vulnerability to cyber-threats is possibly due to the fact that very little information covering the attack is available. One of the most noticeable vulnerabilities to cyber-threats, which can be found in the Norwegian case study, is that of uneducated employees. The malware used in the cyber-attacks on the various oil and gas companies was able to gain access to the different companies' systems because of uneducated employees opening e-mails. If employees were more educated and aware of the risk of cyber-threats, they would be more cautious of opening every e-mail.

The second vulnerability to cyber-threats found in the Norwegian case is the lack of information sharing. Some of the oil and gas companies targeted by a cyber-attack, such as Statoil, acknowledged the risk of cyber-threats following the Shamoon attack. Despite Statoil being aware of the risk of cyber-threats, any plans the company developed to manage or mitigate the new risk of cyber-threats was hindered due to the lack of information sharing about the Shamoon attack. This lack of information sharing points to a third vulnerability to cyber-threats evident in the Norwegian case and that is low cyber-maturity. While Statoil and other companies may have had some form of management plan, they were still impacted. This indicates that while they acknowledged the risk of cyber-threats the company's cyber-maturity is still relatively low.

The fourth and final vulnerability to cyber-threats in the Norwegian case is the reputational risk. Much like the Saudi Aramco case, Statoil has close ties to the Norwegian government and acts as a large source of revenue to the government. Both these close ties and the fact that Statoil is a major contributor to the Norwegian

government's revenue makes the company a viable target for a cyber-attack seeking to cause political or economic upheaval in Norway.

#### **4.4 The Management of Cyber-Threats and Complications with Mitigation**

The oil and gas industry remains to be a vital component of today's world economy and as a result this makes the possibility of completely mitigating the risk of cyber-threats from the industry impossible. This chapter has acted to show how cyber-attacks will not only continue but also increase in the future. The increase of cyber-attacks is especially true for oil and gas facilities located in the Middle East as the risk they face is heightened due to geo-political rivalries (Digitization and cyber disruption in oil and gas, 2017:6). Examples of this heightened risk are already evident in Saudi Aramco's experiences, as we have seen in this chapter with the company being the target of two cyber-attacks. Countries without geo-political rivalries will, however, also experience this same increase due to how lucrative a target the oil and gas industry is. The advancement and the continued introduction of IoT technology will put all aspects of the oil and gas industry at risk from onshore installations, offshore installations, oil tankers and pipelines.

Another factor, which presents a challenge to the mitigation of cyber-attacks on the oil and gas industry, is that they do not follow a distinct pattern. Typically, with traditional methods of attacks a pattern can be discerned due to the attacks typically being connected to periods of political instability in a region that has resulted in oil and gas infrastructure being the target of violent attacks (Giroux & Gilpin, 2013). Cyber-attacks do not tend to follow any particular pattern making them far too unpredictable to track or predict. Cyber-attacks can occur simply to cause a disruption at an oil and gas facility without there being any reason or motivation behind the attack. Such an example is the cyber-attack on Statoil, where no group ever took responsibility for the attack and no motivation was provided. Attacks can also be the result of a hacker testing the capabilities of their malware on a facility. Ultimately, cyber-attacks may not be able to occur at the same frequency due to how much planning and technological knowledge is needed to put together a successful cyber-attack.

A further factor, which complicates the possibility of mitigating cyber-threats against the oil and gas industry, is the world's dependence on oil and gas. Various countries around the world are dependent on the revenue created through exporting oil and gas. This is true for both Saudi Arabia and Norway as both Saudi Aramco and Statoil are the biggest contributors to government revenue. As result, targeting oil and gas infrastructure with cyber-attacks provides the opportunity to directly influence governments and their international partners. The world's reliance shows no sign of decreasing but rather progressively increasing which will only see cyber-attacks against the oil and gas industry increasing along with it. Ultimately, cyber-attacks against oil and gas installations will remain the best way to destabilise Western economies, which as stated in Chapter One is the primary goal of terrorist groups.

The US has been moving towards attempting to import less oil and instead produce it themselves. In 2018, however, the US imported roughly 9.93 million barrels of oil per day. This means the US economy will still be influenced by cyber-attacks on oil and gas facilities. This chapter has established that cyber-attacks seeking to disrupt the US economy can happen on US soil as seen with cyber-attacks on pipelines. On the other hand, countries in Europe are just as vulnerable to the cyber-threats - maybe more so. This increased vulnerability is particularly concerning because Europe's dependence on oil and gas is expected to drastically increase by 2035. This increased dependence only makes Europe oil and gas facilities a bigger target of cyber-attacks.

Essentially, the oil and gas industry are going to continue to be a very lucrative industry and thus will continue to be a target of cyber-attacks. The number of cyber-attacks is only going to increase as new technology continues to be introduced to the infrastructure of oil and gas facilities. New technology will only continue to make the oil and gas industry more vulnerable. It is important to also remember that cyber-attacks have not reached their full potential and will also only grow in sophistication, that will see them become more deadly. The attack surface for cyber-attacks is only going to increase due to increased investment in the oil and gas industry, which will result in more oil and gas installations being built. Building these new installations will only create more points of vulnerability that can be targeted by cyber-attacks.

#### **4.5 Risk Management Recommendations for the Oil and Gas Industry**

As has been established through current research and recent history discussed in this chapter, the oil and gas industry has been and will continue to be one of the largest targets of cyber-attacks. Thus, it is absolutely crucial for risk management plans against cyber-threats to become the biggest priority of the oil and gas industry. The prioritisation of addressing the risk of cyber-threats needs to start at the executive level of oil and gas companies and filter down to the other business units. However, as has been established in looking at the cyber-attacks on Saudi Aramco and Statoil there is a lack of understanding and awareness about cyber-threats and how to manage the risk. For this reason, this research study will briefly present some recommendations which will improve the ability of oil and gas companies to identify and manage future cyber-threats to their facilities. Before making these recommendations, it is very important to be aware that there is no one-size fits all approach to managing cyber-threats against oil and gas companies.

The first recommendation is that awareness amongst employees needs to increase. Oil and gas companies need to start promoting cyber-security awareness amongst their employees and at all levels of the companies. In addition to raising employees' awareness, oil and gas companies need to start training their employees by instilling in them the skills required to interact safely, securely and responsibly. In training employees, it will provide them with the know-how to deal with an attack as quickly as possible.

The second recommendation is to put in place technological methods of risk management that can act as safeguards against cyber-threats. One suggestion is the employment of early warning and detection systems of cyber-threat breaches. Early warning systems provide oil and gas companies with the time necessary to ready themselves to manage the threat of a cyber-attack. The benefit of an early warning system is evident in the cyber-attack on the Norwegian oil and gas companies. A second suggestion is that oil and gas companies should start to deploy anti-malware reputation servers in order to supplement traditional, signature-based anti-virus software normally used at facilities. As was seen in the Stuxnet attack prior to the Shamoon attack, malware of cyber-attacks can easily by-pass traditional anti-virus software. Anti-



malware reputation servers will assist in monitoring for malware that bypasses traditional anti-virus software and alerts the company of this. A final suggestion is isolating potential attack surfaces through separating the business systems from operational systems. As was shown in the Shammoon attack on Saudi Aramco, the company's separation of their corporate network from their operational systems hindered the attack from disrupting oil production and exploration.

The third recommendation for the management of cyber-threats is that oil and gas companies must continuously focus on the risk of cyber-threats. Cyber-threats are constantly evolving and changing, and this is happening at an increasingly faster pace, much like the development and improvement of technology. Today's cyber-threats facing the oil and gas industry may not be the same as those facing the industry in a few weeks' time. In order to effectively manage the risk of cyber-threats evaluation needs to be conducted continuously in order to detect any form of breach or inaccuracy in a facilities' system. This can be done through the use of anti-malware software and hiring of a cyber-security firm to run security checks.

The fourth and final recommendation is that oil and gas companies need to start sharing information with one another with regards to their experiences with cyber-threats and steps they may have taken to manage the threat. It is understandable that some governments, such as Saudi Arabia's, are unwilling to share information about their experience with cyber-threats due to the critical importance of the oil and gas infrastructure to their economy. Withholding this information, however, is only contributing to the lack of awareness about the risk of cyber-threats facing the industry. Oil and gas companies need to start sharing information in order for them to start effectively managing the risk of cyber-threats. Some oil and gas companies have moved toward sharing information to develop management strategies such as the joint project started by DNV GL with Shell, Lundin, Siemens, Honeywell, ABB, Kongsberg Maritime and Statoil.

#### **4.6 Conclusion**

Cyber-threats against the oil and gas industry have a very clear influence. While there have not been many well-documented cases of cyber-attacks against the oil and gas

industry, the influence that they have on the industry cannot be questioned. Cyber-threats have the ability to influence oil and gas production in significant ways. As was seen in the Shamoon attack, Saudi Aramco experienced a halt in their business operations. The attack also stopped their payment methods from working, which resulted in seventeen days of domestic oil trucks waiting to refill and eventually saw the company giving oil away for free. This acts to show that cyber-threats can have an economic impact on countries. In the case of the cyber-attack on Statoil researchers could not identify any clear impact of the attack but it did act to demonstrate that even oil and gas facilities located in areas considered secure are vulnerable to the threat. Additionally, Statoil had risk management strategies in place that were focused on cyber-threats but were still able to be breached. The fact the company was still breached demonstrates that the oil and gas companies cannot mitigate cyber-threats. While cyber-threats are a risk that all international oil and gas companies are going to have to accept, regardless of where they are located, they can start to develop plans to manage the risk of cyber-threats. Oil and gas companies need to start sharing information with one another if they wish to effectively manage the influence of cyber-threats to the industry

## Chapter Five: Conclusion and Evaluation of the Research Study

### 5.1 Introduction

It has become essential for oil and gas companies to take into consideration political risks before investing in a new oil field or even in their daily operations. Oil and gas companies monitor and assess these risks through political risk analysis. For a long time, the biggest political risk facing the oil and gas companies has been terrorism, but this is slowly changing with the introduction of new forms of political risk. The types of political risk that exist are constantly evolving and changing along with changes and trends in global society which has seen the introduction of the political risk of cyber-threats. Cyber-threats are considered to be a political risk of the twenty-first century as a result of the rapid development of technology. In chapter one, the main research question was stated as: “Do cyber-threats increase the political risk which oil and gas companies face?” This question can now be answered accordingly.

While the oil and gas companies have been targets of cyber-attacks, the industry as a whole has been slow to recognise and address the threat they pose. This is due to the fact that executives of oil and gas companies did not believe cyber-threats were a credible threat and would rather focus on protecting their facilities from physical attacks. The cyber-attacks on Saudi Aramco and on Norwegian oil and gas companies have established cyber-threats as a credible threat to the oil and gas industry. These cyber-attacks indicate that cyber-threats ultimately do increase the risk for the oil and gas industry. As well as showing that even oil and gas facilities located in areas considered to be low risk can fall victim to cyber-attacks. Attention is now turning to identifying vulnerabilities to cyber-threats. The vulnerabilities to cyber-threats act as risk indicators. These vulnerabilities are exploited by hackers when they launch a cyber-attack. Through identifying these vulnerabilities, oil and gas companies can start to develop new management strategies to address cyber-threats as they have already proved to have a significant influence on oil and gas companies. If oil and gas companies are slow to implement management strategies, they will continually fall behind in protecting their facilities. This stems from the fact that cyber-threats are rapidly changing and being improved regarding their capabilities.

This chapter provides the conclusion of this research study by providing an overview of progress in relation to the research questions as well as in terms of achieving the aims and objectives of this study. This chapter will additionally provide an evaluation of the research and conclude with recommendations for further studies in cyber-threat risk in relation to the oil and gas industry.

## **5.2 Progress of the Research Study**

In Chapter One the research study was introduced, which was followed by a short literature review. This short literature review focused on areas that are relevant to this research study. This literature review included articles that covered the subjects of political risk and industry-specific risk. Literature, which covered cyber-threats and cyber-attacks on the oil and gas industry, were also covered. This ended with literature that dealt with two cyber-attacks that have occurred in the oil and gas industry, the attack on Saudi Aramco and the attack on Statoil. The main research question, as well as three sub-questions were presented in order to further support the main research question. The following were outlined and discussed: the objectives and relevance of this study, the research design and research methodology and the limitations of the research study were also presented and outlined. The chapter concluded with an outline of the research study.

The primary purpose of Chapter Two was to provide the theoretical grounding necessary for this research study as well as to contextualise the key concepts of the study. The theoretical grounding is based on rational-choice theory, as well as problem-solving and decision-making theory that provided this research study with a framework to work from. Other central concepts to this research study were clarified in this chapter including risk, political risk, macro and micro risk, industry and firm specific risk, risk management and mitigation and lastly cyber-threats. Through examining and expanding on these central concepts this chapter further built on the framework to provide a solid foundation on which this research study could build in Chapters Three and Four.

Chapter Three sought to contextualise the influence that cyber-threats have on the international oil and gas industry. In order to provide this contextualisation, an insight

into the oil and gas industry's utilisation of automation, technological innovations; and the use of IoT was examined. The examination of the utilisation of these aspects is done in order to provide an understanding of how the industry environment has changed and essentially opened themselves up to the rising threat of cyber-attacks. In order to identify vulnerabilities that act as indicators of risk to cyber-threats the three sectors of the oil and gas industry (upstream, midstream and downstream) were examined individually. Through examining these sectors individually different vulnerabilities were identified in each sector as well as the different sectors experiencing different levels of impact. Identifying the different vulnerabilities provided valuable information for the analysis of Chapter Four.

Chapter Four utilised the information presented in Chapter Three as a lens to analyse the cyber-attacks on Saudi Aramco and Statoil. Analysing the cases provided insight into the influence cyber-threats have on the oil and gas industry. This chapter also answered the sub-question utilised to supplement and improve on the quality of analysis. This chapter also scrutinised the ability of oil and gas companies to either be able to mitigate the threat of cyber-attacks or only be able to manage them.

### **5.3 Main Findings of the Research**

The primary objective of this research study was to find out whether or not cyber-threats increase the political risk facing oil and gas companies. It is a recent development that at this point has not reached its full potential but is already evident. Despite it being evident that there is lack of awareness and literature covering the topic of risk of cyber-threats facing the oil and gas industry. The purpose of this study was to increase the knowledge about the risk of cyber-threats to the oil and gas industry, as well as examine whether or not they increase the political risk for the industry. The main research question of this research study is: "Do cyber-threats increase the political risk which the oil and gas companies face?". In order to fully answer this question theory, which was presented in Chapter Two and Chapter Three have been used to examine Chapter Four. The case studies of the cyber-attacks against Saudi Aramco and Statoil provided a much deeper understanding of how cyber-threats increase the political risk faced by oil and gas companies.

Cyber-threats have only recently been identified as a political risk. As such research on the cyber-threats as a political risk to the oil and gas companies is limited due to it being a new phenomenon. As cyber-threats are considered to be a political risk it essentially does increase the political risk faced by oil and gas companies. The Shamoon attack on Saudi Aramco showed how the cyber-attack affected the company in a significant way. Saudi Aramco was forced to shut down the corporate operations in order to recover and were forced to use significant financial revenue to recover as well as give oil away to local trucks to maintain domestic oil supply. Ultimately, while the company did try to recover quickly and despite the company stating that they had recovered shortly after the attack, it actually took the company over two months to fully recover. This shows that cyber-attacks against the oil and gas companies do influence them in more than one way.

The first sub-question asked to support the main research was: “Which risk indicators of cyber-threats can be identified by oil and gas companies in order to help them manage and/or mitigate this threat?” The findings of this research have found that there are numerous indicators of risk identified in the vulnerabilities to cyber-threats that exist throughout the oil and gas industry. Until recently not much attention had been paid to the risk of cyber-threats to the oil and gas industry and thus new vulnerabilities are continually being identified or changing. In Chapter Three of this research study vulnerabilities to cyber-threats in the oil and gas industry were identified and outlined in Table 3.1. These identified vulnerabilities were used as a lens to look at the case studies of this research study and if there was a correlation between them. While some of the identified vulnerabilities were found in both cases not all of them were present. Four of the vulnerabilities identified in Chapter Three were identified in both case studies and were as follows: lack of information sharing, low cyber-maturity, uneducated employees and reputational risk. Identifying these vulnerabilities are key to aiding oil and gas companies in developing plans to either mitigate or manage cyber-threats.

The second sub-question asked was, “Will cyber-attacks result in oil and gas companies losing revenue and halt their daily operations?”. While there have been few well-documented cases of cyber-attacks on oil and gas companies the Shamoon attack on

Saudi Aramco provided insight into answering this question. While Saudi Aramco did not have to halt their daily operations of oil and gas exploration other operations were halted. The business operations of the company were halted as they were trying to fix the computers infected by the cyber-attack. In order to fix the infected hard-drives Saudi Aramco were forced to use substantial financial resources to buy hard-drives from the computer manufacturing floors. Additionally, due to the shutdown of their corporate network the company's payment systems were down which saw miles upon miles of domestic trucks lining up and waiting to be filled. Eventually, Saudi Aramco were forced to give the oil away for free which means the company lost out on a significant amount of revenue from their domestic market. While this answer is limited to the case of Saudi Aramco it does act to show that oil and gas companies do stand to lose revenue and experience a halt in production if they were to be the target of a cyber-attack.

The third and final sub-question was, "Can international oil and gas companies actually mitigate the risk of cyber-threats or is this risk something that can only be managed?". The findings of this research study have revealed that it would be almost impossible for the oil and gas companies to mitigate the risk of cyber-threats. Oil and gas company's inability to mitigate the risk of cyber-threats stems from the fact that much of the world economy is still very much driven by oil and gas. The world's economy's continued dependence on oil and gas means that the companies who produce the commodity will remain targets of cyber-attacks. Another reason oil and gas facilities will continue to be targets of cyber-attacks is the fact that some countries are extremely dependent on the revenue generated by oil and gas exports. This dependency acts to explain why the industry is a prime target of cyber-attacks from terrorist groups or nation-states. It is becoming increasingly more important for companies to start developing management strategies to address cyber-threats. Both the cyber-attacks on Saudi Aramco and the cyber-attack on Statoil clearly demonstrate how serious the threat of cyber-attacks is to the industry. In the case of Saudi Aramco, they had no clear plan in place to effectively manage the threat and had not put into place risk management plans to prevent the attack from happening. This resulted in them using considerable financial resources to recover from the attack. If they had, had management strategies in place, they could have better protected themselves from the influence of the cyber-attack. While it may not be possible for oil and gas companies to fully mitigate the risk of cyber-threats,

companies will need to accept the consequences and start to increase their focus on managing the risk of cyber-threats.

#### **5.4 Evaluation of the Research Study**

The oil and gas industry face numerous risks and will only continue to encounter more in the future. For a long time, the most concerning risk facing oil and gas companies was the threat of terrorism. Oil and gas companies have had to accept this risk due to the fact that they have continually been forced to invest in regions considered to be high-risk. Oil and gas companies have invested in these areas because fewer and fewer new sources of oil reserves are being discovered and those that are, are located in these higher-risk regions thus making companies more vulnerable to terrorist attacks. However, this threat landscape is changing with the introduction of cyber-threats. Cyber-threats do not just put oil and gas facilities located in high-risk regions at risk but even those located in low-risk regions. The purpose of this research study was to analyse whether or not cyber-threats increased the political risk oil and gas companies face. In order to support the research question the upstream, midstream and downstream operations were looked at individually to identify how various operations were influenced and what vulnerabilities to cyber-threats exist. The research question was further supplemented by the chosen case studies of the cyber-attacks on Saudi Aramco and the cyber-attack on Norwegian oil and gas companies, with specific focus on Statoil. These cyber-attacks were selected, as they are the most well documented attacks against the oil and gas industry, as well as the most serious. Both cases displayed how oil and gas companies will face increased political risk as a result of cyber-threats, as well as oil and gas companies only being able to manage cyber-threats.

When it comes to the field of political risk there is a continued lack of consensus on how political risk is defined. Political risk definitions continually range from general to specific. To add to the difficulty in defining political risk, the concept is continually evolving and changing due to global events and trends as well as technological developments. This evolution is evident in the introduction of new forms of political risk that had previously not existed before. In order to address the complexity of political risk and select a suitable definition for this research study, numerous definitions were identified and analysed which provided an informed conceptualisation



of the term. As well as helping provide the most suitable definition of political risk for the twenty-first century. The chosen definition of political risk identified cyber-threats as a form of political risk facing companies. The field of cyber-threats is complex, wide-ranging and very new. Defining cyber-threats is just as difficult due to the evolving nature of the field, as well as a lack of consensus regarding how the concept should be defined. Through examining different definitions, a clear definition was identified which was used together with the selected definition of political risk to provide the foundation for the rest of this research study.

One of the biggest challenges this research study faced was the lack of information available be it primary data or secondary data. Information covering the cyber-attacks Saudi Aramco and Statoil was limited to a few academic articles and newspaper articles. Often these articles merely repeated the same information. International oil and gas companies have never given out detailed information regarding their risk management strategies due to security concerns. This is also true for oil and gas companies' risk management strategies regarding cyber-threats as publishing them would be counter-intuitive and would inform hackers how to circumvent security measures. Risk management companies are just as unwilling to provide access to their management plans. Advisory branches of companies such as Deloitte and Ernst and Young provide models of risk management through their experience of working with oil and gas companies as well as independent research. They published these findings with the purpose of educating the oil and gas industry and providing a deeper understanding of the risk and dangers of cyber-threat to the industry. Other sources such as academic articles and newspapers and surveys done among some oil and gas companies were used to supply the primary data required for this research study.

### **5.5 Recommendation of Further Research**

Political risk is a very complex concept with numerous sub-fields and is continuously developing. For a long time, the older definition of political risk has been utilised to define the concept but there are new definitions which acknowledge new forms of political risk in the twenty-first century. Cyber-threats are a key example of a new form of political risk that has only now been identified as a political risk. As cyber-threats have only been recently identified as a form of political risk, it is extremely under-

researched in comparison to the political risk of terrorism. The connection of cyber-threats to political risk needs to be expanded especially as it is considered to be a rising threat to numerous industries ranging from the medical industry to the oil and gas industry.

A second recommendation concerns research being conducted on risk management in the oil and gas industry in regard to cyber-threats. In order to be able to identify how oil and gas companies manage the risk of cyber-threats, further primary research is needed. Field analysis of oil and gas companies' risk management of cyber-threats would provide a better understanding and insight into how companies manage the risk. Interviews with personnel in charge of risk units in oil and gas companies would provide valuable insight into how these threats are managed. Additionally, primary research conducted on hackers would provide for a more in-depth understanding of hackers' motivations and the methods of how they develop the malware used in cyber-attacks. This in-depth understanding would also assist in informing risk management of cyber-threats to international oil and gas companies. More extensive primary data would provide for a deeper understanding and knowledge, which would serve to help better understand the risk cyber-threats posed to the oil and gas industry.

The Shamoon attack on Saudi Aramco was one of the worst and most well documented cyber-attacks on an oil and gas company. The attack acted as the first visible warning about the oil and gas industries' vulnerability to cyber-attacks. Yet literature remained low and overall awareness amongst companies was limited. The Triton attack in 2017 had a deadly goal, which resulted in greater attention being paid to the threat and resulted in changes being made. Example of changes can be seen by Saudi Aramco entering into a joint partnership with Raytheon to develop methods to secure the oil and gas industry from cyber-attacks. Similarly, two years following the cyber-attack on the fifty oil and gas companies on Norway saw DNV GL initiate a joint venture with numerous companies with the aim of developing methods to manage the risk of cyber-threats. A third recommendation for further research would be to analyse whether or not these changes and new focus on cyber-threats is just a temporary move or if it has actually resulted in a long-term change in risk management in the oil and gas industry.

## 5.6 Conclusion

Addressing the risk of cyber-threats is going to become increasingly more important for the oil and gas companies. It is going to be the biggest threat facing oil and gas companies in the future. Cyber-threats are not only of concern to oil and gas facilities in high-risk areas but even those located in lower risk areas. Cyber-threats are going to become more deadly and seek to cause explosions at facilities and this will put employees' safety at risk. Failing to address this threat can result in severe consequences, as well as a significant loss of revenue be it from trying to recover from the attack or from different operations coming to a halt. This research study has contributed to drawing greater attention to the rising risk of cyber-threats to the oil and gas industry. It has demonstrated the importance of oil and gas companies developing effective management strategies to minimise the influence of cyber-threats. Despite there being documented cyber-attacks against oil and gas companies the industry has been slow to address the issue of cyber-threats and how to manage them. The oil and gas industry will continue to be targets of cyber-attacks in the future but if the oil and gas companies start to develop effective risk management strategies, they can minimise the influence of these attacks. The more cyber-attacks on the oil and gas industry are analysed the better they will be explained and thus better understood which will allow companies to better manage the risk.

## Bibliography

- 300 oil companies hacked in Norway. 2014. [Online]. Available: <https://www.thelocal.no/20140827/norwegian-oil-companies-hacked> [2019, August 15].
- Ahmad, R. & Yunos, Z. 2012. A Dynamic Cyber Terrorism Framework. *International Journal of Computer Science & Information Security*, 10(2), February:149-158.
- Al-Saud, N.B.A. 2012. A Saud Outlook for Cybersecurity Strategies: Extrapolated From Western Experience. *Joint Force Quarterly*, (64):74-81.
- Alon, I. & Herbert, T.T. 2009. A Stranger in a Strange Land: Micro Political Risk and Multinational Firm. *Business Horizons*, 52(2):127-137.
- Alon, I. & Martin, M.A. 1998. A Normative Model of Macro Political Risk Assessment. *Multinational Business Review*, 6(2):10-19.
- Alon, I., Gurumoorthy, R., Mitchel, M.C. & Steen, T. 2006. Managing Mircopolitical Risk: A Cross-Sector Examination. *Thunderbird International Business Review*, 48(5):623-642.
- Arquilla, J. & Ronfelt, D. (eds.). 2001. *Networks and Netwars: The Future of Terror, Crime and Military*. Santa Monica: RAND Corporation.
- Automation in Oil and Gas Industry*. 2018. [Online]. Available: <https://ww2.frost.com/frost-perspectives/automation-oil-and-gas-industry/> [2019, August 15].
- Baldi, S., Gelbstein, E. & Kurbalija, J. 2003. *Hactivism, Cyber-Terrorism and Cyber-war: The Activities of the Uncivil Society in Cyberspace*. Malta: DiploFoundation.

- Becker, C.L. 2013. *Den største trusselen mot olje-og gassindustrien vår* [Online]. Available: <https://www.dn.no/-den-storste-trusselen-mot-olje-og-gassindustrien-var/1-1-1947996> [2019, August 15].
- Beggs, C. 2005. Cyber-Terrorism: A Threat to Australia, in M. Khosrow-Pour (ed.). *Managing Modern Organization Through Information Technology*. Alberta: Idea Group Inc. 472-475.
- Berlin, A., Berlin, A.I. & Vrooman LLP. 2003 Managing Political Risk in the Oil and Gas industries. *Oil, Gas & Energy Law Intelligence* [Electronic], 1(2). Available: <http://d.yimg.com/kq/groups/3862917/1676412124/name/Managing%20Political%20Risk%20in%20the%20Oil%20and%20Gas%20Industries.pdf> [2019, August 15].
- Black Hat Amsterdam: Oil & Gas cyber-vulnerabilities*. 2015. [Online]. Available: <https://www.scmagazineuk.com/black-hat-amsterdam-oil-gas-cyber-vulnerabilities/article/1479359> [2019, August 15].
- Boman, K. 2015. *Fulcher: Cybersecurity Ranks as Top Long-Term Threat to Statoil* [Online]. Available: [https://www.rigzone.com/news/oil\\_gas/a/141595/fulcher\\_cybersecurity\\_ranks\\_as\\_top\\_longterm\\_threat\\_to\\_statoil](https://www.rigzone.com/news/oil_gas/a/141595/fulcher_cybersecurity_ranks_as_top_longterm_threat_to_statoil) [2019, August 15].
- Bray, J. 2003. Attracting Reputable Companies to Risky Environments: Petroleum and Mining Companies, in I. Bannon & P. Collier (eds.). *Natural Resources and Violent Conflict: Options and Actions*. Washington DC: World Bank. 287-352.
- Bremmer, I. & Keat, P. 2009. *The Fat Tail, The Power of Political Knowledge For Strategic Investing*. New York: Oxford University Press.
- Brink, C.H. 2004. *Measuring Political Risk*. Aldershot: Ashgate Publishing Limited.

- Bronk, C. & Tikk-Ringas, E. 2013. The Cyber Attack on Saudi Aramco. *Survival: Global Politics and Strategy*, 55(2): 81-96.
- Bronk, C. & Tikk-Ringas, E. 2013. Hack or Attack? Shamoan and the Evolution of Cyber Conflict. Working Paper, James A. Baker III Institute For Public Policy, Rice University [Online]. Available:  
<https://www.bakerinstitute.org/media/files/Research/dd3345ce/ITP-pub-WorkingPaper-ShamoanCyberConflict-020113.pdf> [2019, August 15].
- Bronk, C. 2016. *Cyber Threat: The Rise of Information Geopolitics in U.S. National Security: The Rise of Information Geopolitics in U.S. National Security*. United States of America: ABC-CLIO.
- Bryne, M. 2014. *Hackers Launch All-Out Assault on Norway's Oil and Gas Industry* [Online]. Available:  
[https://motherboard.vice.com/en\\_us/article/bmjdm/d/hackers-target-300-norwegian-oil-and-energy](https://motherboard.vice.com/en_us/article/bmjdm/d/hackers-target-300-norwegian-oil-and-energy) [2019, August 15].
- Brynjar, L. 2005. *Globalisation and the Future of Terrorism*. London: Routledge.
- Burnham, P., Lutz, K.G., Grant, W. & Layton-Henry, Z. 2008. *Research Methods in Politics*. New York: Palgrave Macmillan.
- Butler, K.C. & Joaquin, D.C. 1998. Political Risk and the Return on Foreign Direct Investment. *Journal of International Business Studies*, 29(3):599-607.
- Carpenter, J.W. 2015. *The Biggest Oil Producers in Africa* [Online]. Available:  
<https://www.investopedia.com/articles/investing/101515/biggest-oil-producers-africa.asp> [2019, August 20].
- Chicken, J.C. 1986. *Risk Assessment for Hazardous Installations*. Oxford: Pergamon Press.

- Choucri, N. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press.
- Clark, N., Abraham, A. & Goyal, S. 2016. *Improving oil and gas efficiency through digital* [Online]. Available: <https://www.strategyand.pwc.com/report/improving-oil-gas-efficiency-digital> [2019, August 15].
- Cordesman, A.H. & Obaid, N. 2005. *National Security in Saudi Arabia: Threats, Responses, and Challenges*. United States of America: Greenwood Publishing Group, Inc.
- Cybersecurity for Oil and Gas Industries: How Hackers Can Manipulate Oil Stocks, 5 March 2016 [Video file]. Available: <https://www.youtube.com/watch?v=NPdARknmJ4E> [2019, August 15].
- de Borchgrave, A., Cillufo, F.J., Cardash, S.L. & Ledgerwood, M.M. 2000. *Cyber Threats and Information Security Meeting the 21<sup>st</sup> Century Challenge*. Washington, D.C.: Center for Strategic and International Studies (CSIS).
- Deering, D. & Sweeney, G. 2017. Understanding the Scope: Brief History of Energy Industry Cyberattacks. *Pipeline & Gas Journal*, 244(5), May:65-67.
- Dehlawi, Z. & Abokhodair, N. 2013. Saudi Arabia's response to cyber conflict: A case study of the Shamoon Malware incident, *IEEE International Conference on Intelligence and Security Informatics (ISI)*. 4-7 June, Seattle, United States of America. Los Alamitos, California: IEEE Computer Society [Electronic]. Available: <https://ieeexplore.ieee.org/document/6578789> [2019, August 15].
- Denning, D.E. 2000. *Cyberterrorism* [Online]. Available: <http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf> [2019, August 16].

- Denning, D.E. 2001. Activism, Hacktivism, and Cyberterrorism, in J. Arquilla & D. Ronfeldt (eds.). *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica: Rand Corporation. 239-288.
- Denning, D.E. 2007. A View of Cyberterrorism 5 Years Later, in K.E. Himma (ed.). *Internet Security: Hacking, Counterhacking, and Society*. United States of America: Jones Bartlett Publishers, Inc. 123-139.
- Digitization and cyber disruption in oil and gas*. 2017. [Online]. Available: [https://www.ey.com/Publication/vwLUAssets/ey-wpc-digitization-and-cyber/\\$FILE/ey-wpc-digitization-and-cyber.pdf](https://www.ey.com/Publication/vwLUAssets/ey-wpc-digitization-and-cyber/$FILE/ey-wpc-digitization-and-cyber.pdf) [2019, August 16].
- DNV GL. 2016. *Technology Outlook 2025*. [Norway]: Erik Tanche Nilssen [Online] Available: <https://to2025.dnvgl.com/energy/oil-gas/> [2019, October 9].
- Dragonfly: Western Energy Companies Under Sabotage Threat*. 2014. [Online]. Available: <https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear> [2019, October 9].
- Eaton, C. 2017a. Hacked: As cyberattacks become more sophisticated energy industry's controls provide an alluring target. *Houston Chronicle* [Electronic], 2 March. Available: <https://www.houstonchronicle.com/news/houston-texas/houston/article/As-cyberattacks-become-more-sophisticated-energy-10973429.php> [2019, August 16].
- Eaton, C. 2017b. Hacked: Put to the test, cybersecurity experts infiltrate energy companies' networks. *Houston Chronicle* [Electronic], 2 March. Available: <https://www.houstonchronicle.com/business/article/Put-to-the-test-cybersecurity-experts-easily-10989830.php> [2019, August 16].



*Energy Charting Tool*. 2016. [Online]. Available: [http://tools.bp.com/energy-charting-tool.aspx?&\\_ga=2.240320131.1295978284.1494852322-1342952496.1494852322#/st/oil/dt/rp/unit/Years/region/NOA/SCA/EU/MIE/AFR/AP/view/column/](http://tools.bp.com/energy-charting-tool.aspx?&_ga=2.240320131.1295978284.1494852322-1342952496.1494852322#/st/oil/dt/rp/unit/Years/region/NOA/SCA/EU/MIE/AFR/AP/view/column/) [2017, May 17].

European Union Agency For Network and Information Security. 2017. *Report on Cyber Security Information Sharing in the Energy Sector*. [Electronic] 1(1). Available: <https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector> [2019, August 31].

Fineren, D. & Bakr, A. 2012. *Saudi Aramco says most damage from computer attack fixed* [Online]. Available: <https://www.reuters.com/article/net-us-saudi-aramco-hacking/saudi-aramco-says-most-damage-from-computer-attack-fixed-idUSBRE87P0B020120826> [2019, August 16].

Fitzpatrick, M. 1983. The Definition and Assessment of Political Risk in International Business: A Review of the Literature. *The Academy of Management*. 8(2):249-254.

Frynas, J. G. & Mellahi, K. 2003. Political risks as firm-specific (dis)advantages: Evidence on transnational oil firms in Nigeria. *Thunderbird International Business Review*, 45(5):541-565.

Giroux, J. & Gilpin, R. 2013. Tackling Energy Infrastructure Vulnerability in Violence Prone Zones. *Journal of Energy Security*. [Online]. Available: <http://www.fletcherforum.org/home/2016/8/22/tackling-energy-infrastructure-vulnerability-in-violence-prone-zones> [2019, August 16].

Gordon, S. & Ford, R. 2003. *Cyberterrorism? (White paper)* [Online]. Available: <https://www.symantec.com/avcenter/reference/cyberterrorism.pdf> [2019, August 16].

- Green, S. 2002. *Rational Choice Theory: An Overview*. Seminar on Rational Choice. Baylor University. [Online]. Available: [http://business.baylor.edu/steve\\_green/green1.doc](http://business.baylor.edu/steve_green/green1.doc) [2019, August 30].
- Groll, E. 2017. Cyberattack Targets Safety System at Saudi Aramco. *Foreign Policy* [Online], 21 December. Available: <https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/> [2019, August 19].
- Grom, C. 2018. *N.J. gas attendant pocketed \$300k by hacking gas pump computers, police say* [Online]. Available: [https://www.nj.com/union/2018/06/police\\_sly\\_nj\\_gas\\_attendant\\_hacked\\_gas\\_pump\\_comput.html](https://www.nj.com/union/2018/06/police_sly_nj_gas_attendant_hacked_gas_pump_comput.html) [2019, August 16].
- Haendel, D. 1979. *Foreign Investments and the Management of Political Risk*. Boulder: Westview.
- Heidar, T. 2016. *65% of oil and gas companies unprepared against major cyberattack: Results are still troubling, but awareness is growing* [Online]. Available: [https://www.fox-it.com/en/about-fox-it/corporate/news/65-oil-gas-companies-unprepared-major-cyberattack/?set\\_hide\\_cookiemessage=yes](https://www.fox-it.com/en/about-fox-it/corporate/news/65-oil-gas-companies-unprepared-major-cyberattack/?set_hide_cookiemessage=yes) [2019, August 16].
- Helgesen, O.K. 2013. *Prøver å lamme oljeproduksjon med cyberangrep: Statoil følger nøye med* [Online]. Available: <https://www.tu.no/artikler/prover-a-lamme-oljeproduksjon-med-cyberangrep/232713> [2019, August 16].
- Hiralal, N. 2017. *Wielding the Double Edged Sword in The Cyber Domain- The Utility of Internet Securitisation in Countering Islamic State Cyberjihad*. Unpublished master's thesis. Stellenbosch: Stellenbosch University.
- Hough, M. 2008. *An Introductory Context of the Methodological, Conceptual, and Theoretical Framework of Risk Analysis*, in K.G. Adar, R.O. Iroanya & F.

Nwonwu (eds.). *Towards Africa-Orientated Risk Analysis Models: A Contextual and Methodological Approach*. Pretoria: Africa Institute of South Africa. 1-17.

Hotvedt, S.K., Aardal, E., Lauritzen F. & Kristoffersen E.B. 2014. 50 norske bedrifter utsatt for dataangrep [Online]. Available: <https://www.nrk.no/norge/dramatisk-auke-i-dataangrep-1.11899596> [2019, August 15].

Hsieh, L. 2015. Drilling cybersecurity: Industry recognizing need for better cyber defences as hackers become more sophisticated and drilling equipment becomes more interconnected. *Drilling Contractor* [Online], 8 September. Available: <http://www.drillingcontractor.org/drilling-cybersecurity-36727> [2019, August 16].

ICT Data and Statistics Division. 2015. *ICT Facts and Figures – The world in 2015*. Geneva: International Telecommunication Union.

Jakobsen, J. 2012. *Political Risk and the Multinational Company: Concepts, Theories and Evidence*. Trondheim: Tapir Akademisk Forlag.

Janbu, A.F. 2016. *Olje-og gassindustrien går sammen I kampen mot cyberkriminalitet* [Online]. Available: <https://www.dnvgi.no/news/olje-og-gassindustrien-gar-sammen-i-kampen-mot-cyberkriminalitet-77263> [2019, August 19].

Johansen, P.A. & Færaas, A. 2014. Hackergruppen Dragonfly mistenkt for å stå bak tidenes norske hackerangrep: Gruppen som har drevet storstilte angrep siden 2011 kan være de som prøver å infisere norske oljeselskaper. *Aftenposten* [Online], 27 August. Available: <https://www.aftenposten.no/norge/i/J1Lpb/Hackergruppen-Dragonfly-mistenkt-for-a-sta-bak-tidenes-norske-hackerangrep> [2019, August 16].

- Johnson, M. 2016. *Cyber Crime, Security and Digital Intelligence*. New York: Routledge.
- Kaplan, S. & Garrick, B.J. 1981. The Quantitative Definition of Risk. *Risk Analysis*, 1(1): 11-27.
- Keane, J. 2015. *The Internet of Things Is Making Oil Production Vulnerable to Hacking* [Online]. Available: [https://www.vice.com/en\\_us/article/qkjpkd/the-internet-of-things-is-making-oil-production-vulnerable-to-hacking](https://www.vice.com/en_us/article/qkjpkd/the-internet-of-things-is-making-oil-production-vulnerable-to-hacking) [2019, August 15].
- Kobrin, S.J. 1979. Political Risk: A Review and Reconsideration. *Journal of International Business Studies*, 10(1):67-80.
- Kobrin, S.J. 1980. Foreign Enterprise and Forced Divestment in LDCs. *International Organization*, 34(1):65-88.
- Kobrin, S.J. 1981. Political Assessment by International Firms: Model or Methodologies?. *Journal of Policy Modelling*, 3(2):251-270.
- Krauss, C. Cyberattack Shows Vulnerability of Gas Pipeline Network. *The New York Times* [Online], 4 April. Available: <https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html> [2019, August 16].
- Lachow, I. 2009. Cyber Terrorism: Menace or Myth, in F.D. Kramer, S.H. Starr & L.K. Wentz (eds.). *Cyberpower and National Security*. Washington, DC: National Defence University Press. 437-464.
- Lambrechts, D. & Blomquist, L.B. 2016. Political-security risk in the oil and gas industry: the impact of terrorism on the risk management and mitigation. *Journal of Risk Research*, 1-18.

- Lambrechts, D., Weldon, C. & Boshoff, M.J. 2010. Political Insecurity and the Extraction Industry in the Democratic Republic of Congo: Moving towards an Industry Specific Political-Security Risk Analysis Mode, in Swart, G. (ed.). *A Vanquished Peace? Prospects for the Successful Reconstruction of the Congo*. London: Adonis & Abbey Publishers Ltd.
- Lax, H.L. 1983. *Political Risk in the International Oil and Gas Industry*. Green's Farms: Atlantis, Inc.
- Lewis, J.D. 2014. *The Islamic State: A Counter-Strategy for a Counter-State*. Middle East Security Report 21. Washington, DC: Institute for the Study of War.
- Leyden, J. 2014. *Major cyber attack hits Norwegian oil industry: Statoil, the gas giant behind Scandic social miracle, targeted* [Online]. Available: [https://www.theregister.co.uk/2014/08/27/norwegian\\_oil\\_hack\\_campaign/](https://www.theregister.co.uk/2014/08/27/norwegian_oil_hack_campaign/) [2019, June 17].
- Lia, B. & Kj ok,  . 2004. Energy Supply as Terrorist Targets? Patterns of Petroleum Terrorism, 1968-99, in D. Heradstveit & H. Hveem (eds.). *Oil in the Gulf: Obstacles to Democracy and Development*. Aldershot: Ashgate. 100-124.
- Luft, G. & Korin, A. 2003. *Terror's Next Target*. [Online]. Available: <http://www.iags.org/n0111041.htm> [2017, August 20].
- Lutz, B.J. & Lutz, J.M. 2015. Globalisation and Terrorism in the Middle East. *Perspectives on Terrorism*, 9(5), October:27-46.
- McAfee Foundstone Professional Services and McAfee Labs. 2011. *Global Energy Cyber-attacks: "Night Dragon" (White Paper)* [Online]. Available: [https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee\\_NightDragon\\_wp\\_draft\\_to\\_customersv1-1.pdf](https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf) [2019, August 16].

- Middle East oil and gas is prime target for cyber attack*. 2019. [Online]. Available: <https://www.offshore-technology.com/comment/middle-east-oil-and-gas/> [2019, August 16].
- Miller, K.D. 1992. A Framework for Integrated Risk Management in International Business. *Journal of International Business Studies*, 23(2):311-331.
- Mittal, A., Slaughter, A. & Zonneveld, P. 2017. *Protecting the connected barrels: Cybersecurity for upstream oil and gas* [Online]. Available: [https://www2.deloitte.com/content/dam/insights/us/articles/3960-connected-barrels/DUP\\_Protecting-the-connected-barrels.pdf](https://www2.deloitte.com/content/dam/insights/us/articles/3960-connected-barrels/DUP_Protecting-the-connected-barrels.pdf) [2019, August 16].
- Morris, C. 2018. *Hackers Have a New Favorite Target: Gas Stations* [Online]. Available: <https://fortune.com/2018/07/09/hackers-gas-stations/> [2019, August 19].
- Munson, L. 2014. *Massive cyber attack on oil and energy industry in Norway* [Online]. Available: <https://nakedsecurity.sophos.com/2014/08/28/massive-cyber-attack-on-oil-and-energy-industry-in-norway/> [2019, August 19].
- Muller, L.P., Gjesvik, L. and Friis, K. 2018. *Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector*. Norway: Norwegian Institute of International Affairs.
- Nagpal, R. 2002. Cyber Terrorism in the Context of Globalisation, *II World Congress on informatics and Law*. [Electronic]. Available: <https://www.asianlaws.org/aboutus/spain.pdf> [2019, August 19].
- Nakashima, E. 2012. Iran acknowledges that Flame virus has infected computers nationwide. *The Washington Post* [Online], 29 May. Available: [https://www.washingtonpost.com/world/national-security/iran-acknowledges-that-flame-virus-has-infected-computers-nationwide/2012/05/29/gJQAzlEF0U\\_story.html](https://www.washingtonpost.com/world/national-security/iran-acknowledges-that-flame-virus-has-infected-computers-nationwide/2012/05/29/gJQAzlEF0U_story.html) [2019, August 19].

- Nakashima, E., Miller, G. & Tate, J. 2012. U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. *The Washington Post* [Online], 19 June. Available: [https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV\\_story.html](https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html) [2019, August 19].
- National Academy of Sciences. 1991. *Computers at Risk: Safe Computing in the Information Age*. Computer Science and Telecommunications Board. Washington, DC.: National Academy Press.
- Negroponte, J.D., Palmisano, S.J. & Segal, A. 2013. *Defending an Open, Global, Secure and Resilient Internet*. Independent Task Force Report No. 70. New York: Council in Foreign Relations
- Neuwman, W.L. 2014. *Social Research Methods, Qualitative and Quantitative Approaches*. United States of America: Pearson.
- Oil and gas cybersecurity: Penetration testing techniques*. 2014. [Online]. Available: [http://www.ey.com/Publication/vwLUAssets/Oil\\_and\\_gas\\_cybersecurity\\_-\\_Penetration\\_testing\\_techniques/\\$FILE/EY-O&G\\_cybersecurity-penetration\\_testing\\_techniques.pdf](http://www.ey.com/Publication/vwLUAssets/Oil_and_gas_cybersecurity_-_Penetration_testing_techniques/$FILE/EY-O&G_cybersecurity-penetration_testing_techniques.pdf) [2019, August 27].
- Operation "Oil Tanker": The Phantom Menace*. 2015. [Online]. Available: <https://www.pandasecurity.com/mediacenter/src/uploads/2015/05/oil-tanker-en.pdf> [2019, August 19].
- Pagliery, J. 2015. The inside story of the biggest hack in history. *CNN Business* [Online], 5 August. Available: <https://money.cnn.com/2015/08/05/technology/aramco-hack/> [2019, August 19].

- Perlroth, N. 2012. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. *The New York Times* [Online], 23 October. Available:  
<https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?auth=login-google> [2019, August 19].
- Perlroth, N. & Krauss, C. 2018. A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. *The New York Times* [Online], 15 March. Available:  
<https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html> [2019, August 19].
- Pollitt, M.M. 1998. Cyberterrorism – Fact or Fancy?. *Computer Fraud & Security*, (2):8-10.
- Polyakov, A. 2016. *Oil and Gas Cyber Security Basics* [Online]. Available:  
<https://erpscan.com/press-center/blog/oil-gas-cyber-security-basics/> [2018, August 26].
- Polyakov, A. 2017. Cyber Security Risks To Be Aware Of In The Oil And Gas Industries. *Forbes* [Online], 3 April. Available:  
<https://www.forbes.com/sites/forbestechcouncil/2017/04/03/cyber-security-risks-to-be-aware-of-in-the-oil-and-gas-industries/#396375b33f0a> [2019, August 29].
- Rashid, F.Y. 2015. *Inside the Aftermath of the Saudi Aramco Breach* [Online]. Available:  
<https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676> [2019, August 19].
- Reed, S. 2019. Saudi Aramco Is World's Most Profitable Company, Beating Apple by Far. *The New York Times* [Online], 1 April. Available:  
<https://www.nytimes.com/2019/04/01/business/saudi-aramco-profit.html>  
[2019, August 29].



- Rice, C. & Zegart, A. 2018. *Political Risk: How Businesses and Organizations Can Anticipate Global Insecurity*. New York: Twelve.
- Rick, K. & Iyer, K. 2016. *Countering the Threat of Cyberattacks in Oil and Gas* [Online]. Available: [http://image-src.bcg.com/Images/BCG-Countering-the-Threat-of-Cyberattacks-in-Oil-and-Gas-Mar-2016\\_tcm9-186245.pdf](http://image-src.bcg.com/Images/BCG-Countering-the-Threat-of-Cyberattacks-in-Oil-and-Gas-Mar-2016_tcm9-186245.pdf) [2019, October 9].
- Roberts, J. 2012. *Cyber threats to energy security, as experienced by Saudi Arabia* [Online]. Available: [https://blogs.platts.com/2012/11/27/virus\\_threats/](https://blogs.platts.com/2012/11/27/virus_threats/) [2019, October 9].
- Robertson, J. & Riley, M. 2014. *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar* [Online]. Available: <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar> [2019, October 9].
- Robock, S.H. 1971. Political Risk Identification and Assessment. *Columbia Journal of World Business*, 4:6-20.
- Robock, S.H. & Simmonds, K. 1989. *International Business and Multinational Enterprises (4<sup>th</sup> edition)*. Homewood, IL: Irwin.
- Rollins, J. & Wilson, C. 2007. *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*. Congressional Research Service Report for Congress [Online]. Available: <https://fas.org/sgp/crs/terror/RL33123.pdf> [2019, October 9].
- Sanger, D. E. 2018. Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute. *The New York Times* [Online], 23 October. Available: <https://www.nytimes.com/2018/10/23/us/politics/russian-hackers-saudi-chemical-plant.html?rref=collection%2Fbyline%2Fdavid-e.-sanger> [2019, October 9].

- Shattuck, T., Slaughter, A. & Zonneveld, P. 2017. *Refining at risk: Securing downstream assets from cybersecurity threats: A Report by Deloitte Center for Energy Solutions* [Online]. Available: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/energy-resources/deloitte-uk-di-refining-at-risk.pdf> [2019, October 9].
- Shaw, M. 2018. *Known unknowns: the threat of cybercrime in Africa: New technology is rapidly turning Africa into a source, and a target, of cybercrime* [Online]. Available: <https://issafrica.org/iss-today/known-unknowns-the-threat-of-cybercrime-in-africa> [2019, October 9].
- Shoot, B. 2018. *Beware Credit Card Skimmers at Gas Stations This July Fourth, Secret Service Warns* [Online]. Available: <https://fortune.com/2018/07/03/gas-pump-credit-card-skimmers-secret-service-warning/> [2019, October 9].
- Simon, H.A. 1982. Political Risk Assessment: Past Trends and Future Prospects. *Columbia Journal of World Business*, 17(3):62-70.
- Simon, H.A. 1955. Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, 69(4):99-118.
- Simon, H.A. 1979. Rational Decision Making in Business Organizations. *The American Economic Review*, 69(4):493-513.
- Simon, H.A., Dantzig, G.B., Hogarth, R., Plott, C.R., Raiffa, H., Schelling, T.C. Shepsle, K.A., Thaler, R., Tversky, A. & Winter, S. 1987. Decision-making and problem-solving. *Interfaces*, 17(5):11-31.
- Slaughter, A., Bean, G. & Mittal, A. 2015. *Connected barrels: Transforming oil and gas strategies with the Internet of Things. A report by Deloitte Center for Energy Solutions* [Online]. Available:

[https://www2.deloitte.com/content/dam/Deloitte/in/Documents/energy-resources/in-enr-Deloitte\\_Es\\_Energia\\_DUP-Internet-of-Things-for-OilGas.pdf](https://www2.deloitte.com/content/dam/Deloitte/in/Documents/energy-resources/in-enr-Deloitte_Es_Energia_DUP-Internet-of-Things-for-OilGas.pdf)  
[2019, October 9].

Stohl, M. 2006. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, Law and Social Change*, 46(4):223-238.

*Storage Terminals need protection against cyber attacks*. 2018. [Online]. Available: <http://www.oilandgastechology.net/news/storage-terminals-need-protection-against-cyber-attacks> [2019, October 9].

*Terrorist Attack and Threats in Algeria*. 2016. [Online]. Available: <https://www.graphiq.com/vlp/adLVEuemrUV> [2019, October 9].

*The Cyber Security Threat to the Oil & Gas Industry*. 2017. [Online]. Available: <https://www.pwc.co.uk/oil-gas/assets/cyber-inoil-and-gas-graphic.pdf> [2019, October 9].

Thomson, J. 2017. Automation In The Oil Industry: What's Next For One Of The Big Players. *Forbes* [Online], 31 May. Available: <https://www.forbes.com/sites/jeffthomson/2017/05/31/automation-in-the-oil-industry-whats-next-for-one-of-the-big-players/#33c82a743ce6> [2019, October 9].

*Timeline: Sanctions on Iran*. 2012. [Online]. Available: <https://www.aljazeera.com/news/middleeast/2012/10/20121016132757857588.html> [2019, October 9].

Top Ten Cybersecurity Vulnerabilities for Oil and Gas. 2016. *Pipeline & Gas Journal*, 243(2), February:26-28.

Tversky, A. Kahneman, D. 1986. Rational Choice and the Framing of Decisions. *The Journal of Business*, 59(4):251-278.

- Untitled*. 2012. [Online]. Available: <https://pastebin.com/HqAgaQRj> [2019, October 9].
- Vertzberger, Y.Y. 1998. *Risk Taking and Decisionmaking: Foreign Military Intervention Decisions*. Stanford: Stanford University Press
- Wagstaff, J. 2014. *All at sea: global shipping fleet exposed to hacking threat* [Online]. Available: <https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140423> [2019, October 9].
- Weimann, G. 2004a. *Cyberterrorism: How Real Is the Threat?*. Special Report 119. Washington, DC: United States Institute of Peace.
- Wells, L.T, 1998. God and Fair Competition: Does the Foreign Direct Investor Face Still Other Risks in Emerging Markets? In T.H. Moran (ed.). *Managing International Political Risk*. Malden: Blackwell Publishers Ltd. 15-43.
- Wilhoit, K. & Hilt, S. 2015. *The GasPot Experiment: Unexamined Perils in Using Gas-Tank- Monitoring Systems* [Online]. Available: <https://www.blackhat.com/docs/us-15/materials/us-15-Wilhoit-The-Little-Pump-Gauge-That-Could-Attacks-Against-Gas-Pump-Monitoring-Systems-wp.pdf> [2019, October 9].
- Wilkinson, P. 2003. Why Modern Terrorism: Differentiating Types and Distinguishing Ideological Motivations, in C.W. Kegley, Jr (ed.). *The New Global Terrorism: Characteristics, Causes, Controls*. New Jersey: Prentice Hall. 106-150.
- Yetiv, S. 2011. *The Petroleum Triangle, Oil, Globalization, and Terror*. New York: Cornell University Press.

Zonneveld, P. & Slaughter, A. 2017. *An integrated approach to combat cyber risk: Securing industrial operations in oil and gas* [Online]. Available: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/intergrated-approach-combat-cyber-risk-oil-gas.pdf> [2019, October 9].

Zetter, K. 2012. *Qatari Gas Company Hit With Virus in Wave of Attacks on Energy Companies* [Online]. Available: <https://www.wired.com/2012/08/hack-attack-strikes-rasgas/> [2019, October 9].