The Identification and framing of cybersecurity threats in South Africa

By

Student Number: 14316472

Thalia Avvakoumides

A mini-dissertation submitted in partial fulfilment of the requirements for the degree

Master of Security Studies (MSS)

Prepared under the supervision of Mr Roland Henwood

Department of Political Sciences

Faculty of Humanities

University of Pretoria

May 2022

Declaration of originality

DECLARATION OF ORIGINALITY

UNIVERSITY OF PRETORIA

The Department of Humanities places great emphasis upon integrity and ethical conduct in the preparation of all written work submitted for academic evaluation.

While academic staff teach you about referencing techniques and how to avoid plagiarism, you too have a responsibility in this regard. If you are at any stage uncertain as to what is required, you should speak to your lecturer before any written work is submitted.

You are guilty of plagiarism if you copy something from another author's work (eg a book, an article or a website) without acknowledging the source and pass it off as your own. In effect you are stealing something that belongs to someone else. This is not only the case when you copy work word-for-word (verbatim), but also when you submit someone else's work in a slightly altered form (paraphrase) or use a line of argument without acknowledging it. You are not allowed to use work previously produced by another student. You are also not allowed to let anybody copy your work with the intention of passing if off as his/her work.

Students who commit plagiarism will not be given any credit for plagiarised work. The matter may also be referred to the Disciplinary Committee (Students) for a ruling. Plagiarism is regarded as a serious contravention of the University's rules and can lead to expulsion from the University.

The declaration which follows must accompany all written work submitted while you are a student of the Department of Political Sciences. No written work will be accepted unless the declaration has been completed and attached.

Full names of student: Thalia Avvaloumides

Student number: 14316472

Topic of work: The Identification and framing of Cybersecurity threats in South Africa

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.
2. I declare that this dissertation (eg essay, report, project, assignment, dissertation, thesis, etc) is my own original work. Where other people's work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.
3. I have not used work previously produced by another student or any other person to hand in as my own.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

SIGNATURE Thalia

Acknowledgements

I would like to take this opportunity to express my utmost gratitude to Mr. Roland Henwood, Sophia, George, Savvas and Dorothy Avvakoumides, Lambo Demetriou and Sanet Oberholzer.

First of all, to my dedicated and understanding supervisor, Mr. Roland Henwood. Finalising this study, would not have been possible if it were not for all your guidance. Please accept my sincerest thanks for all your support during the course of my Master's degree.

Second, thank you to my God parents Sophia Avvakoumides and George Avvakoumides for opening your house to me during a period of my studies and for going above and beyond to ensure that I continue my studies regardless of challenging circumstances. To my dear father Savvas Avvakoumides, thank you for your unwavering support and always being there for me every step of the way – no matter how long it has taken me. I hope that this study makes you proud. Thank you for always encouraging me to further my education. Thank you to my mother Dorothy Avvakoumides for all your encouragement and support. I appreciate everything beyond measure.

Thank you to my phenomenal boyfriend Lambo Demetriou for your unconditional support. Additionally for supporting my dreams and pushing me to continue, even when the end felt out of reach. I quite literally would not have been able to complete this study if it was not for you – you have supported me through every challenge along the way and for that I will always be grateful.

Thank you to my editor Sanet Oberholzer. Your keen eye contributed significantly to this study.

Abstract

This study outlines and defines relevant concepts related to cybersecurity threats. Additionally, the study proposes an amended framework that adapts and combines key concepts utilised in Hare (2010) and Dunn Cavelty's (2015) analytical frameworks, and in turn, applies the amended framework to identify how cybersecurity threats are framed in South Africa. The study finds that cybersecurity threats in South Africa are framed as cybercrime threats to computer networks and business networks. Similarly, this study concludes that South African policy makers conceive cybersecurity threats to be "criminal activities in cyberspace" as proposed by Hare (2010 :218). This study contributes to current knowledge on cybersecurity threats in the Political Sciences field and further contributes to knowledge on cybersecurity threats in South Africa and therefore, paves the way for future studies.

Keywords: cybersecurity threats, cybersecurity, South Africa, identification, framing, Forrest Hare, Dunn Cavelty, analytical framework

List of Abbreviations

Abbreviation	Full term
ARMSCOR	Armaments Corporation of South Africa
CERTS	Computer Emergency Response Team
CSIR	Centre for Scientific and Industrial Research
CSIRT	Computer Security Incident Response Team
DoS	Denial of service
DDoS	Distributed denial of service
ICT	Information and communications technology
SANDF	South African National Defence Force
SAPS	South African Police Service
SARS	South African Revenue Service
SITA	State Information Technology Agency
SSA	State Security Agency

Table Of Contents

Chapter One: Research Overview

1.Focus of the study

Cyberspace has introduced a new dimension to national security, and additionally introduced contemporary cybersecurity threats to computer, business, government and military networks. The protection of cyberspace is therefore necessary as it is all-encompassing of a state's political, social, financial, and military spheres. Although the securitisation of cyberspace is arguably a global issue, as the domain transcend the boarders of any one country. It is however apparent that policymakers within a state frame the securitisation of certain cybersecurity threats, by use of threat narratives.

To illustrate this point, this study fundamentally explores the identification and framing of cybersecurity threats in South Africa, "through the narratives associated with these types of threats"(Maness & Valeriano 2016: 262). The main focus of this study is to provide exploratory research on the cybersecurity threat discourse in South Africa. This study therefore outlines and defines relevant concepts related to cybersecurity and cybersecurity threats. Lastly ,as a means to explore cybersecurity threat framing in South Africa the analytical frameworks of Hare (2010) and Dunn Cavelty (2015) are utilised.

1.2 Formulation and demarcation of the research problem

The research problem identified in this study, is that there is a gap in Security Studies academic literature addressing the identification and framing of cybersecurity threats in South Africa. This type of research is significant as states have varying perspectives of cybersecurity threats. For that reason, conceptualising cybersecurity threats in a South African context allows for exploratory research that identifies the framing of the concept in a particular country. South Africa suffers from a shortage of cybersecurity professionals, indicating a cybersecurity skills gap in the country. In lieu of this fact, and to address the research problems identified in this study, the study bridges the gap between a technical understanding of cybersecurity threats and offers a Security Studies interpretation of these threats which is inclusive of analytical Security Studies analytical frameworks, therefore offering a humanities interpretation of cybersecurity

threats within a South African context while remaining inclusive of the technical conceptualisations associated with cybersecurity threats.

1.3 Literature review

In order to understand cybersecurity threat in the context of this study, the study will examine previous definitions provided by scholars from the realist, liberalist, and constructivist fields before arriving at why Critical Security Studies frameworks are most applicable to this study and formulating the most up to date assumptions of cybersecurity threats which is all-encompassing of the issues in the 21st century.

Contrary to Bay's (2016: 2) assumption that the broadness of the concept of cybersecurity poses challenges for theoretical exploration, multiple studies have been conducted applying various Political Sciences lenses to cybersecurity and cybersecurity threats. This literature review will discuss how cybersecurity threats have been conceptualised in the three most popular main theoretical perspectives: realism, liberalism, and constructivism and, in turn, will expand on which of these perspectives has influenced the work of Dunn Cavelty and Hare.

Realist scholars such as Thomas Hobbes and Nicolo Machiavelli argue that the state is a central unit of analysis. Realist scholars predominantly apply a military definition of security and therefore consider information warfare to be an element of inter-state conflict in the way electronic jamming of communication was used in WW2 as a type of electronic warfare. Traditional Security Studies scholars have placed technology, specifically military hardware, at the forefront of technology and security. However, the rise of cybersecurity threats such as cyberwarfare and cyberespionage has changed the way in which realist scholars understand security and technology. Although the state remains the referent object in need of securitisation from a cybersecurity threat, military force cannot protect a state from these types of threats.

Liberal scholars such as Immanuel Kant, Adam Smith, and John Maynard Keynes make the assumption that international actors and non- state actors remain essential in light of domestic and political factors in a country. These factors guide the manner in which states conduct themselves internationally. However, in relation to

cybersecurity, this relates to pursuing cybernorms through platforms such as the United Nations. According to Eriksson and Giacomello (2006: 229), liberal theorists view cybersecurity threats to be directly related to the expansion of technology through the process of globalisation. For liberal scholars, technological advancement has impacted the way in which states ensure national security and how cybersecurity threats have entered into existence. Further, the rise of non-state actors directly impacted how liberal scholars view cybersecurity threats. This is evident through conceptions of cybersecurity threats such as cyberterrorism, hacktivism, and cyberespionage.

Various political sciences lenses are used to conceptualise cybersecurity threats. The most prominent theoretical lens identifiable from the literature is constructivism, which directly links to securitisation theory (Nissenbaum 2005; Hansen & Nissenbaum 2009; Hare 2010; Dunn Cavelty 2015). Constructivism offers one of many interpretations of cybersecurity threats and accounts for diverse discourses associated with cybersecurity threats. This is subject to rhetoric regarding cybersecurity threats which, in turn, is subject to the influence of social construction. Futter (2018) reiterates that cybersecurity threats are constructs and are essentially viewed in the "eye of the beholder." Constructivism is a lens in which all cybersecurity threats can be viewed and conceptualised. It accommodates for cybersecurity threats to be understood from multiple discourses and from differing national perspectives.

National perceptions play a significant role in how specific cybersecurity threats are framed. Lewis (2014) identifies national perceptions of cyberthreats and claims that certain events shape perception, for example the incident that occurred in Estonia or the Stuxnet worm. In these cases, cyberattacks occurred at such astronomical levels that they attracted international attention as well as increased concern regarding cybersecurity and cyberattacks which may threaten the critical national infrastructure of a country. Cyberattacks of such significance contributed to the framing of cybersecurity threats as these incidents were politicised and therefore directly influenced national security discussions regarding cybersecurity on a global level. In this sense, merging cyberspace with the concept of cybersecurity is undoubtedly considered to be a political action (Liebetrau & Christensen 2020: 3).

Constructivist perspectives remain the most relevant lens for this study, as constructivist theory scholars such as Buzan, Wilde and Waever believe in the critical examination of threat perceptions. Securitisation theory is the starting point to understanding the creation of threats, yet there are many contesting views or frameworks on threat creation. Securitisation theory acts as a foundational theory for both Dunn Cavelty and Hare's frameworks. A critical examination of a threat is conducted through the application of securitisation theory to a referent object. Securitisation theory originated from the Copenhagen school and evaluates how, when, and why political actors frame something as a matter of security.

Constructivist analysis correlates with the conceptualisation of intrinsic value attached to rhetoric and symbolic actions. Ontological assumptions made about securitisation theory by scholars from the Copenhagen School suggest that threats are constructed. The process which a threat undergoes in order to be considered securitised is fundamentally subjective. Specific rhetorical structures understood as 'speech acts' play a significant role in framing political issues as security threats (Buzan *et al*. 1998: 36). Fundamentally, a narrative is established by a state's elites to express and justify why something is a threat in need of immediate action.

Securitisation theory's ontological assumptions made by scholars from the Copenhagen School suggest that threats are constructed through a systematic process involving speech acts, securitising actors, a securitising move, a referent object, de-securitisation, sectors of security, facilitating conditions, and an audience (Buzan *et al*. 1998: 20). The process that a threat undergoes in order to be securitised is subjective as a narrative need to be established, expressing why something is considered a security threat. Nevertheless, there is a clear theoretical trend identifiable in the range of literature written on cybersecurity threats.

Further, the application of Buzan *et al*. 1998 "Security: A New Framework for Analysis" is used as a theoretical framework by multiple leading voices in cybersecurity discourses. For example, Nissenbaum (2005: 66) provides a valuable framework for articulating differences between conceptions of security in cybersecurity and technical computer security. Whereas Hansen and Nissenbaum's (2009) article "Digital disaster, cybersecurity, and the Copenhagen school" adopts securitisation as a

framework, the study fundamentally expresses distinct sectors with particular constellations of threats and referent objects. These referent objects are state, society, and economy, articulated to be threatened through the different types of securitisations such as hyper-securitisation, everyday cybersecurity practices, and technifications.

Previously published academic literature on the topic cybersecurity threats in the context of South Africa can be broken down into the following themes. The first theme evident from the literature is policy orientated focusing on the governance of cybersecurity in South Africa. The second theme is cybersecurity threats as a national security threat. Lastly, South Africa's response to the cyber threat.

Dunn Cavelty and Hare's frameworks allow for one to determine the identification and framing of cybersecurity threats. It needs to be stipulated that although Dunn Cavelty and Hare are not South African scholars both authors provide valuable analytical frameworks and have made efforts to conceptualise cybersecurity threats from a security studies lens, which in turn makes their analytical frameworks valuable to this study.

1.4 Research question

The research question for this study is: "How does combining Dunn Cavelty's and Hare's analytical frameworks inform the identification and framing of cybersecurity threats in South Africa?" This research question guides the study and hones in on evaluating the value of both analytical frameworks.

1.5. Aim and objectives

The overarching aim of this study is to understand the identification and framing of cybersecurity threats in South Africa. In order to achieve the overarching aim of this study, three objectives are proposed:

- To define, describe, and explain key concepts that contribute to the understanding of cybersecurity threats;
- To evaluate Dunn Cavelty (2015) and Hare's (2010) frameworks;

- To apply Dunn Cavelty's (2015) and Hare's (2010) analytical frameworks to South Africa's cybersecurity threat landscape.

1.6 Scope of the study

This study is conducted from a Security Studies perspective and focuses on the identification and framing of cybersecurity threats within South Africa.

1.7 Research methodology

This study applies a qualitative approach to cybersecurity threats. In line with a qualitative approach, the study is a literature-based study and is inclusive of application of analytical frameworks from Hare (2010) and Dunn Cavelty (2015). In order to address the research problem of this study, the analytical frameworks proposed by Hare (2010) and Dunn Cavelty (2015) are adapted to develop a analytical framework which is applicable to South Africa. A critical literature-based method is suitable for this study as it "goes beyond a mere description of identified articles and includes a degree of analysis and conceptual innovation" (Grant & Booth 2009: 93). In addition, this method allows for the critical review of both Dunn Cavelty (2015) and Hare's (2010) frameworks and allows one to test the applicability of these frameworks to the context of South Africa.

This study utilises both primary and secondary evidence. The types of data used in this study include e-books, internet sources, electronic newspaper sources, electronic journals, as well as governmental reports, bills, acts, and speeches delivered in South Africa regarding cybersecurity threats. The data used is available in the public domain.

1.8 Limitations and ethical considerations

A limitation to this study is access to data. Some information regarding cybersecurity threats may not be available to the public as it is considered to be sensitive. The study is conducted as a mini-dissertation which limits the scope that may be covered. On the basis that the study will be conducted using literature as a means for data collection, an ethical consideration is that all sources are within the public domain and will be referenced. No human subjects will be utilised for this study.

1.9 Research design

Chapter One: Research overview

This chapter introduces the focus of the study. The study similarly addresses the formulation and demarcation of the research problem, a literature review, research question, and aim and explains the objectives of this study. This chapter states the research methodology, structure, limitations, and ethical considerations of the study.

Chapter Two: Literature review of key concepts

This chapter begins by outlying and exploring definitions of relevant concepts related to cybersecurity threats. The chapter identifies various cybersecurity threat discourses and briefly discusses what these threat discourses entail. The chapter provides a working definition for this study.

Chapter Three: Evaluation of Dunn Cavelty's and Hare's analytical frameworks

This chapter provides an evaluation of both Hare(2010) and Dunn Cavelty (2015) analytical frameworks and proposes an amended framework that adapts Hare (2010) and Dunn Cavelty's (2015) frameworks to explore South Africa's cybersecurity threat landscape.

Chapter Four: The identification and framing of cybersecurity threats in South Africa

This chapter applies the amended analytical framework to the context of South Africa and specifically answers the research question identified in this study. The chapter additionally explores the framing and identification of cybersecurity threats in South Africa.

Chapter Five: Findings, recommendations for future studies, and conclusion

The final chapter consists of findings, recommendations, and a conclusion.

Chapter Two: Literature review of key concepts

2.1 Cyberspace

The "prefix 'cyber' relates to "…all electronic and computer-related activities" (Nye 2010: 3). It is important to note that 'cyber' may be written as a single word or be hyphenated. For the sake of consistency in this study, the prefix 'cyber' will be applied to compound nouns as one word. The origin of the prefix 'cyber' dates back to 1984. However, the concept only entered into physical existence via the World Wide Web in 1980 (Reveron 2012: 5) and thereafter became what we now understand to be the internet. An understanding of cyberspace and what this entails is key to this study, as cybersecurity threats cannot be explored without an understanding of where these types of attacks take place. Despite cyberspace's origin having good intentions designed in order to make information more accessible, it has become apparent that the domain is a realm in which a paradox lies. Harnessing cyberspace is both an opportunity to advance technologically, while allowing for greater vulnerability. This logic applies to individuals, states, and corporates alike. This man-made domain has changed the notion of threats, as threats now wield a cyber-related element and anyone is considered to be fair game when cyberattacks are launched. Whereas in the past there were geographical factors involved, cyberspace now transcends borders and in turn allows for the access of information to no longer require extravagant ploys.

Defining cyberspace is a challenging task. Singer and Friedman (2013: 21) point out that "the reason why cyberspace is so difficult to define, lies not only in its expansive global nature but also in the fact that the cyberspace of today is almost unrecognisable compared to its humble beginnings." A second reason justifying why defining cyberspace remains to be a challenge is rooted in the way in which states choose to govern the use of cyberspace. To illustrate this point, China has repeatedly expressed that cyberspace is a legitimate domain for warfare, whereas the United States believes that the use of cyberspace is beneficial to fundamental freedoms such as freedom of speech, and in turn, is a platform designed to allow for greater opportunities related to commerce, communication, and an exchange of ideas. These challenges highlight the complex nature of creating norms which govern cyberspace, and similarly the different uses for the platform.

Multiple reasons exist for why cyberspace definitions remain challenging. However, Joseph Nye provides a sound definition of cyberspace, which succinctly identifies what cyberspace is inclusive of. This definition expresses the entirety of the domain: cyberspace comprises of both physical and virtual dimensions as “cyberspace includes not only the internet of all networked computers, but also intranets, cellular technologies, fibre-optic cables, and space-based communication” (Nye 2010: 19). Given the fact that cyberspace is a man-made domain, it is subject to framing by political entities. On this basis, the domain is further considered to be classified as a historical and political phenomenon.

The nexus between cyberspace and national security is complex. A state does not have monopoly in cyberspace and the prevalence of non-state actors has become more apparent in recent years. An incredibly concerning reality is that the information environment is considered to be a domain in which legitimate military activities occur (Reveron 2012: 4-6). This fact raises huge concern for states, corporates, and citizens as data has become increasingly valuable and can therefore be considered the main commodity influencing geopolitics today (Jarmon & Yannakogeorgos 2018). sThe exponential growth of cyberspace has created a conducive environment for cybervulnerabilities or threats to multiply. In this regard, there is a need to ensure the protection of this domain. Therefore, cybersecurity is the backbone to securing cyberspace.

2.2. Cybersecurity

The concept ‘security’, similar to the prefix ‘cyber’, is so embedded in our everyday life. Not only do we make decisions based on security concerns, but so do the organisations that we work for, and the states in which citizens reside. Security is, therefore, unavoidably a contested concept (Williams & McDonald 2018: 1) due to the fact that security has broadened and deepened in order to become more inclusive of non- traditional security threats. As such, it is essential to make sense of security before applying the prefix ‘cyber’ to ‘security’, which in turn opens a new dimension of security. The concept security has evolved through the Political Sciences discipline.

The origin of the cybersecurity field can be traced back to 1980 and can be identified through the establishment of the first computer emergency response team, whose core function was to provide coordinated responses to cybersecurity threats. Galinec *et al*. (2017: 273) argue that “cybersecurity has been practised in military circles for over a decade.” Despite using the concept from a military perspective, it was first used in 1990 in the computer security field to illustrate insecurities seen in networked computers. Commercialisation of the internet in the 1990s created an increased magnitude of devices connected to the internet in the 21st century which continues to grow exponentially on a daily basis. Most importantly, the concept of cybersecurity has reached the attention of officials in countries as well as scholars from the International Relations and Security and Strategic Studies fields. As a result, the concept has since gained interest in the role technology plays in national security.

The discipline of Security Studies gained momentum before 1945 and was highly influenced by scholars from America. The theoretical concepts focusing on security have moved away from realist thought towards more reflective thought. For example, Buzan’s (1983) work moved away from the state as the sole referent object and towards the notion of security sectors that he deemed to be priorities. Thereafter the emergence of Critical Security Studies developed as a new lens that rejects viewing security from a realist lens and adopts the notion that security should be broadened and deepened to encompass more security issues (Olivares 2018). As a result of security undergoing a broadening and deepening, the concept has, in turn, become multifaceted, contextual, and – some scholars would argue – socially constructed. These factors allow security to have multiple definitions. Security is most commonly identified as “the alleviation of threats to cherished values; especially those which, if left unchecked, threaten the survival of a particular referent object in the near future” (Williams & McDonald 2018: 6). The following section will explore what attaching the prefix ‘cyber’ to ‘security’ entails and provide a working definition of cybersecurity which is applicable to this study.

There are several reasons why defining cybersecurity is problematic. Firstly, the rise of the concept cybersecurity both as a concept and practice, and its convergences with other forms of security, has hindered definitional consensus and “no one can agree on what cybersecurity means, or what it requires" (Stevens 2018: 1). While

scholars such as Siboni (2013), Dunn Cavelty (2013), and Griffiths (2017: 1) argue that cybersecurity is a national security issue the concept is no longer confined to the realms of national security. With the introduction of social media and smart phones, cybersecurity is no longer limited to the state and corporates as cybersecurity is equally important to the everyday citizen. Furthermore, cybersecurity is not stagnant. What is apparent from the literature on cybersecurity, in the context of Security Studies, is that "while the field of cybersecurity is not new, the intellectual maturity of the perspective is developing" (Maness & Valeriano 2016: 269). As such, cybersecurity needs to be adaptable to a continuously changing threat environment.

Secondly, it is apparent in the literature that the concept has developed an array of diverse interpretations. Nissenbaum (2005: 63) introduces cybersecurity as the "link between computer security and traditional notions of national security." However, in recent years it is apparent that cybersecurity encompasses far more than what Nissenbaum's definition expresses. Nissenbaum's definition only accounts for one cybersecurity discourse identified by Dunn Cavelty in a 2015 article which illustrates diverse interpretations of cybersecurity by identifying three cybersecurity discourses pertaining to a technical focus: cybercrime, cyberespionage, and civil and military spheres. Lastly, Forcepoint (2020) provides a holistic definition of cybersecurity as "the practice of ensuring the integrity, confidentiality, and availability of information." In order to avoid any conceptual confusion and because various scholars define cybersecurity differently, a working definition will be applied to ensure that the definition remains standard throughout this study.

Despite cybersecurity existing in military circles for over a decade and cybersecurity emerging as a technical field in the 1990s, the conception of cybersecurity in the 21st century has changed drastically since its emergence. Firstly, cyberspace emerged when few concerns regarding insecurities were present, as it was designed in the absence of security. Secondly, the commercialisation of the internet has created more vulnerabilities. Dunn Cavelty (2015: 363) expresses cybersecurity's paradoxical nature as it "is both about the insecurity created by and through this new place/space and about the practices or processes to make it more secure." The exponential growth of cyberspace has created a conducive environment for cybervulnerabilities/ threats to multiply similarly, highlighting the need for cybersecurity.

Cybersecurity is multidimensional, not only virtually, but physically too. It is undeniable that the security of cyberspace has been sacrificed for its functionality and now cybersecurity is a means to managing more significant complexities which will continue to arise with the ongoing globalisation of information and an increase in connectivity globally.

Nissenbaum (2005) produced an article titled “Where computer security meets national security” which is the focal point for where cybersecurity and computer security meet. This study is considered a seminal work which explores cybersecurity in relation to computer security. Hansen and Nissenbaum (2009: 1156), on the other hand, “pathed the way for what hyphening security with cyber might imply in Security Studies.” Computer security’s mandate has broadened, creating an array of challenges and concerns regarding this growth. This has proportionately allowed for diversified sophisticated attacks and inundated information which requires protection in societies.

Cybersecurity and technical security have similar aims; however, cybersecurity embodies more. Matthews *et al*. (2016: 35) express that “cybersecurity has truly become a political, military, economic, social, information, infrastructure, physical environment, and time concern for senior leaders.” The concept of cybersecurity is used by a diverse set of actors in the political, computer sciences, tech, health, and national security industries. However, certain discourses of cybersecurity are articulated more so in specific sectors. For example, cybersecurity is articulated more by government authorities as a means to prevent cyberespionage, cyberwar, and cyberterrorism. At the same time, corporate heads will articulate that the notion of cybersecurity plays a role in preventing hacking, cybercrime, and cyberespionage. In light of the COVID-19 pandemic, cybersecurity has become more critical than ever, as employees began working from home and the state’s health sectors have tried to protect their vaccine production from cyberespionage.

Cybersecurity is discussed holistically in this section and comprehensive overview of cybersecurity is achieved which paves the way to understanding cybersecurity threats

2.3. Cybersecurity threats

This section will discuss cybersecurity threats and similarly describe the different types of cybersecurity threats evident from the literature. In order to understand cybersecurity threats holistically, one needs to understand their origin, how they have been defined differently, and the theories used to explore cybersecurity threats. Therefore, to achieve a comprehensive understanding of cybersecurity threats, this section will discuss the term 'cybersecurity threat'.

Our knowledge regarding what classifies as a cybersecurity threat , is informed by technical cybersecurity experts, academic research, political rhetoric, and corporate cybersecurity policies. Although many people do not understand the technical aspects of cybersecurity and cybersecurity threats, political rhetoric regarding cybersecurity threats have shaped their opinions without individuals even realising. For scholars researching cybersecurity threats, previous academic work is what has shaped how cybersecurity threats are studied.

2.3.1 Definitions and characteristics

The concepts cybersecurity threat or cyberthreat can be used interchangeably and both concepts encompass an array of threats. These threats are classified in accordance with different cybersecurity discourses. Therefore, definitions pertaining to cybersecurity threats may vary. The National Institute of Standards and Technology (2021) define cybersecurity threats as:

> *"…any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the State through an information system via unauthorised access, destruction, disclosure, modification of information, and denial of service."*

This definition is inclusive of various cybersecurity threats, which is beneficial to this study. As new cybersecurity threats arise and old threats grow in sophistication, definitions require a holistic approach to defining cybersecurity threats.

The Canadian Centre for Cybersecurity (2021: 2) defines cyberthreats as “cyber activities intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.” A cyberthreat may similarly be referred to as a potential attack in which the objective is to attain unwarranted entry into a server and distort information, intellectual property, or confidential information. According to Lewis (2002), a “cyberthreat’s primary goal is to access computer network tools in order to invoke chaos that has the ability to cripple critical national infrastructures, such as transportation, energy and government operations.” The underlying aim of a cyberthreat is to construct conditions in which fear or financial or physical harm occur. These conditions are created by harnessing a certain level of information through technology (White 2016: 23).

Cybersecurity threats have continued to advance since the first threat was recorded, namely the Markus Hess’ cuckoo egg hacks into several US military and research facilities in 1985 (Gamero-Garrido 2014: v). Cybersecurity threats have commonly been categorised as cyberwarfare, cyberterrorism, cyberespionage, cybercrime, and hacktivism. What makes cybersecurity threats unique is that they are considered asymmetric (Tatar *et al*. 2016: 314). Furthermore, the threats mentioned above may involve multiple methods and various cybertools to achieve these attacks.

It is important to note that cybersecurity threats are essentially possible attacks that may occur. A cyberattack has different characteristics to a cybersecurity threat. Where a cybersecurity threat may or may not be malicious, a cyberattack is intentionally malicious. Cyberattacks are defined as “an attack, via cyberspace, targeting an enterprise’s use of cyberspace to disrupt, disable, destroy, or maliciously control a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information” (Jahankhani *et al.* 2014: 161).

The first cyberattack can be traced back to the Morris Worm. This attack played a significant role in the discovery of a cybertool called a worm which was designed by a researcher named Robert Thomas (Mutune 2021). In 1988 the second worm was created by American graduate Robert Morris. This attack changed how cybersecurity threats were previously conceptualised as its ability to infect 10% of computers illustrated a cybersecurity threat’s capacity for destruction with malicious intent.

Cybersecurity threats have transcended from an academic field into criminal acts (Mutune 2021). The cybersecurity field arose out an interest to explore and conceptualise the vastness of the World Wide Web. However, despite initial good intentions, there are some states, individuals, and organisations that have used cybersecurity's vulnerabilities to promote their own gain. In order to understand cybersecurity threats holistically, conceptualisations of cybersecurity threats are essential.

Jabbour and Devendorf (2017: 79) identify what constitutes a cybersecurity threat through 'cyberthreat characterisation', which is a valuable source to this study as cyberthreats are explained from a technical perspective. Jabbour and Devendorf (2017: 79) define a cybersecurity threat as "the cyber-risk to an information system which is a function of (1) the likelihood of a potential vulnerability, (2) the possibility of a threat exploiting the vulnerability, and (3) the impact of successful exploitation." Three components that are required for an attack to be classified as a cybersecurity threat are "capability, access and intent." These motivations are the driving force for cybersecurity threats to occur.

Futter (2018) offers a different perspective of cybersecurity threats as constructs which are essentially defined in the "eye of the beholder." Futter (2018: 206) argues that cybersecurity threats may refer to any type of cyberattack, ranging from low-level hacking to espionage, existential attacks, and warfare. Therefore, the term 'cyberthreat' may be counterintuitive because it encompasses various attacks and vulnerabilities. Scholars such as Madžarević (2016), Israel and Tabansky (2011), Marsili (2019), and Brangetto and Veenendaal (2016) have diverging perceptions of cybersecurity threats. The very fact that these scholars have diverging perceptions on cybersecurity threats is an indication that cybersecurity threats are not all viewed in the same manner. Further, the diversity of cybersecurity threats indicates the existence of various cybersecurity discourses in which various cybersecurity threats are prioritised (Dunn Cavelty 2015: 40).

According to Futter (2018: 206) and Cornish *et al*. (2021), cybersecurity threats may refer to any type of cyberattack, including low-level hacking, espionage, existential

attacks, and warfare. In the following chapter , these cybersecurity threats will be described and explained: cyberwarfare, cyberterrorism, cyberespionage, cybercrime, and hacktivism.

2.3.3 Common types of cybersecurity threats discourses

a) Cybersecurity discourse

A most commonly discussed cybersecurity threat is the lack of cybersecurity professionals skilled enough in order to manage or mitigate cyberattacks. globally There are a few reasons as to why this type of cybersecurity threat should be classified as just as much of a threat as cyberwarfare, cyberterrorism, cyberespionage, cybercrime, or hacktivism. Firstly, cybersecurity is complex and in turn, requires complex solutions to complicated problems. Due to technological advancement, constant up skilling is required in this type of industry, as cybersecurity attacks are constantly advancing. Secondly, cybersecurity threats need to be understood from multiple disciplines as they impact each and every industry, state, and individual using a connected device. Therefore, these types of threats require various legal, political, technical, and economic investments into building cybersecurity strategies within a state in order to successfully secure the referent objects. As a result, one needs not only technical cybersecurity skills but also an understanding of the whole picture – the ripple effect of a cybersecurity attack, if you will – and its implications. Similarly, it is necessary to understand the motivation behind an attack as the rationale for why an attack occurs is an important factor related to the mitigation of a threat.

b) Cyberwarfare discourse

The rise of information technology has created a new domain in which warfare may occur and Post-Cold War the nature in which wars are fought has changed. Developing countries such as “India and Cuba are believed to be developing cyberwarfare capabilities” and countries such as “Russia, China and the United Kingdom and the United States have incorporated cyberwarfare into their military doctrines” (Baylis *et al*. 2013: 217). Non-state actors have also been introduced as new threat agents.

Cyberwars are fought through tools such as global media perceptions, information, and electronic deception and the amount of disinformation readily available in the 21st century is an example of how easy it is to share disinformation through the internet, social media, and electronic devices. Cyberwarfare also pertains to a "state's ability to attack another state's computer and information network in cyberspace and to protect its capabilities from attacks by adversaries" (Ciolan 2014: 128). Cyberwarfare is defined by Carr (2011) as "the art and science of fighting without fighting; of defeating an opponent without spilling their blood," while Tikk (2011: 58) defines cyberwarfare as "state-level info war in which the attack motivation is for political or military gain and targets infrastructure or military assets." Many scholars refer to this cyberwarfare as what a cyber pearl harbour would look like, and believe that cyberwarfare will not occur (Smith 2013: 82). Cybertools used in order to wage a cyberwarfare attack pertain to the use of malware, phishing, and worms in order to spread disinformation, hold government information for ransom, or wage an attack on a state's critical infrastructure.

The cyberattacks that occurred in Estonia in 2007 and in Iran in 2010 are manifestations of cyberwarfare. In Estonia's case, multiple denial of service (DoS) attacks were launched in order to "overload and crash servers and websites through repeated and simultaneous requests for information carried out by botnets" (Herzog 2011). These attacks impacted financial services at two banks, government websites, and multiple political organisations within the county and illustrated the implications an attack can have on a state. In the Iranian case, the Stuxnet worm used in the attack "disrupted Iranian nuclear enrichment infrastructure in 2010 and caused physical damage across international boundaries" (Herzog 2011). This attack changed the way in which cybersecurity threats are conceptualised and illustrated the increasing need for securitisation. Stuxnet was positioned as the most mechanically modern malignant programme produced for a designated assault to date.

c) Cyberterrorism discourse

Cyberterrorism is the least understood cybersecurity threat. According to Talihärm (2010: 59-73), "there were many voices that doubted it was even a threat" due to how

media perceived the cyberthreat. The concepts of cyberterrorism and cyberwarfare may easily be confused. According to Shipley and Bowker (2014), cyberwarfare differs from cyberterrorism as it is an organised effort by a state to conduct operations in cyberspace against another state, whereas cyberterrorism is essentially "terrorism in cyberspace" (Ciolan 2014: 128). Cyberterrorism entails the attack of communication infrastructure in a state and is orchestrated with either intimidation or by creating fear to pursue a socio-political objective. For an attack to be classified as cyberterrorism, a combination of noteworthy disruption, grievances, and significant economic loss needs to occur (Weimann 2004). Cyberspace has created a new platform in which terrorist organisations can meet, recruit, and wage an attack.

c) Cyberespionage discourse

Cyberespionage, the oldest cyberthreat, is defined as a method of gathering intelligence and information not available in the public domain. Threat agents may be individuals, states, or businesses trying to achieve a monetary advantage or benefit. In cases where government perpetrates a state-sponsored attack, the core objective is rooted in breaking into a system with unauthorised access for the sole purpose of intelligence or data collection pertaining to military power, economic advantage, or a state security. Information communications technology (ICT) has changed the rate at which intelligence collection efforts occur. The cybertools used to wage these attacks are advanced persistent threats, malware, social engineering, spear phishing, and watering hole attacks. The Center for Strategic and International Studies (2021) specialises in reporting "cyber-attacks on government agencies, defence and high-tech companies or economic crimes with losses over millions of dollars" and has reported on global cyberincidents from 2003 to 2021. Their report highlights the rate at which cyberespionage attacks occur globally and they point out that cyberattacks occur more often than perceived. They also note that the role that geopolitics plays in cyberincidents is significant.

d) Cybercrime discourse

There is no universal definition of cybercrime (Payne 2020). Cybercrime involves a range of highly sophisticated organised crime to low-level crime and is considered an

everyday threat to societies. Cybercrime involves various cyberattacks such as phishing, spam, hacking and malware, spyware, and viruses and continues to expand in sophistication and range. Jahankhani *et al*. (2014: 149) take note of transformative keys which have created new avenues for cybercriminals to wage their attacks. These transformative keys are globalisation, distributed networks, synoptics and panopticism, and data trails. The threat of cybercrime encompasses a vast array of virtual and physical criminal activities and the fact that countries have vague explanations of cybercrime becomes problematic as cybercrimes constitute multiple types of attacks, including "phishing, spam, hacking, cyber harassment, identity theft, plastic card fraud and Internet auction fraud. Cyber-attack techniques for cyber-crime involve malware, spyware and viruses" (Jahankhani *et al*. 2014: 148).

e) Hacktivism discourse

Hacktivism originated in 1999. Since then, it has advanced in terms of sophistication. Hacktivists use non-violent cybertools to achieve a range of political, social, religious, and anarchist objectives. The cybertools used by hacktivists include "electronic sit-ins, virtual blockades, automated email bombing, viruses and worms, defacement and spoofing of websites as well as occasional computer system break-ins" (Panda Security 2021). In cases where government entities are targeted, the cybertactics used are DoS, doxxing, or defacement. Recent manifestations of hacktivism are illustrated in the "Black Lives Matter movement, collection of Clinton emails, attack on US executive branch, Project Chanology, Hactivismo declaration and worms against nuclear killers" (Panda Security 2021).

2.3.4 Working definition of cybersecurity threats

A working definition of cybersecurity threat will be formulated that is all-encompassing of this multifaceted phenomenon which can be analysed theoretically across various levels. It is essential to express that, despite the fact that this study will provide a working definition of cybersecurity threat, this definition will not aim to define cybersecurity threat once and for all, nor does it favour a particular lens in which cybersecurity can be viewed. This working definition will indicate that there is, in fact,

a presence of diverse cybersecurities threat, each existing simultaneously as Illustrated by Dunn Cavelty (2015).

Craigen *et al*. (2014: 13) highlight the importance of formulating a working definition that is central to the study at hand. Their methodological craftsmanship which informs this study is two-fold: firstly, by expressing previous definitions of cybersecurity threat discourse and indicating commonalities within those definitions as well as analysing the usefulness of the definitions identified and, secondly, by formulating their own working definition of cybersecurity that is best suited to their study.

As Lewis (2014: 567) explains, “cybersecurity has changed security priorities by identifying the internet and cyberspace as a source of new threats. In many countries, the threat perception is either reactive or determined by exogenous influences.” When formulating a working definition of cybersecurity threats, it is essential to understand the concept holistically, so that one encapsulates the framing of the concept and why multiple cybersecurity threat discourses have arisen. Referring to previous definitions of cybersecurity threat is essential when attempting to create a working definition for a study as academic engagement with the concept of cybersecurity threat plays an intricate role in constructing and shaping the reality of cybersecurity threat. Further, previous definitions allude to which cybersecurity issues were most prominent in specific years and compare what current cybersecurity issues are most prudent.

For the purpose of this mini-dissertation, the working definition of cybersecurity threat is a multi-dimensional phenomenon encompassing differing perceived cyber related attacks. Which is additionally influenced by a constructed view of responding to perceived cyber related attacks. This definition emphasises that cybersecurity is a multi-faceted phenomenon and takes into account cybersecurity threats are perceived threats to referent objected related to individuals, states, or corporations.

Conclusion

In conclusion, the nature of cybersecurity threats has changed gradually over time yet it remains certain that these threats pose tremendous risk to states, corporates, and everyday citizens. Cyberspace is integrated into all spheres of a society, placing cybersecurity threats as a genuine concern all round. This chapter discussed related

definitions, descriptions, and explanations of key concepts to this study. The chapter additionally outlined cybersecurity threat discourses and presented a working definition applicable to this study. The following chapter will discuss Dunn Cavelty and Hare's analytical frameworks and evaluate their applicability to this study.

Chapter Three: Evaluation of Dunn Cavelty's and Hare's analytical frameworks

3.1. Introduction

This chapter sets out to evaluate Dunn Cavelty and Hare's analytical frameworks and the ability of each author to assist in explaining the framing and identification of cybersecurity threats in South Africa. However, before one can successfully apply these analytical frameworks to the South African cybersecurity threat landscape, it is important to understand the concepts used in each analytical framework. Below, the analytical concepts from both Hare and Dunn Cavelty's frameworks will be discussed in relation to this study.

3..2. Key concepts

3.2.1 Actors

Actors are understood in this study as the policymaker, organisation, or government entity responsible for expressing securitisation logic in the technical, crime-espionage, and military cybersecurity discourses.

3.2.2 Referent objects

Referent objects refer to the objects deemed in need of a securitising act.

3.2.3 Information assurance

Information assurance relates to the acceptance that insecurity in cyberspace can never be reduced to zero as there will always be an element of risk.

3.2.4 Technical discourse

The technical discourse is constantly evolving due to constantly new types of cybersecurity threats. The technical discourse encompasses viruses, worms, and other bugs. This discourse lays the foundation for cybercrime and espionage discourse as well as military and civil discourse.

3.2.5 Cybercrime and cyberespionage discourse

Cybercrime discourse refers to crime that involves computers and networks whereas cyberespionage discourse refers to strategic information gathering at a national level or through the use of hacking.

3.2.6 Military and civil discourse

This discourse entails cyberwarfare and cyberterrorism and applies the use of cyberweapons to military power.

3.2.7 Power

Power is understood in this study as the capability of a state's military function to secure the state from threats.

3.2.8 Socio-technological cohesion

Socio-technological cohesion is understood in this study as a method to understand cybersecurity and cybersecurity threat policy within South Africa.

3.3. Dunn Cavelty and Hare's analytical frameworks

3.3.1. Dunn Cavelty

Dunn Cavelty identifies three cybersecurity discourses which encompass the main actors involved in the securitisation process of referent objects within these cybersecurity discourses. Dunn Cavelty's study further identifies which cybersecurity threats are classified under relevant cybersecurity discourses. The first discourse identified by Dunn Cavelty (2015: 401-406) is a technical focus, the second is the inter-relationship between cybercrime and cyberespionage, and the third is military and civil defence wars in the information domain and critical infrastructure protection. Dunn Cavelty, like many Critical Security Studies scholars, focuses on a context approach to studying how cybersecurity is made up of certain constructions and performed in different social spheres by focusing on the conducive conditions that have allowed certain cybersecurity discourses to emerge. Essentially, this assists in understanding which conditions have allowed for the development of cybersecurity threats and, in turn, the securitisation of cybersecurity.

Dunn Cavelty (2015: 365) is adamant that “cybersecurity is highly politicised and that risk perceptions are dependent on institutions and emotions as well as perceptions of experts,” reiterating that cybersecurity is what politicians, technical experts, and media want it to be. Depending on certain types of states, the pursuit of securing cyberspace allows the state to infringe on human rights. By suggesting that cybersecurity is framed in such a way, it seems irrefutable that a state has the authority to regulate the use of cyberspace in its territory.

In summary, Dunn Cavelty’s 2015 article encompasses a national security approach towards understanding cybersecurity and highlights the security issue of cyberinsecurity. The focus in Dunn Cavelty’s article is to express “why cybersecurity is considered one of the key national security issues of our time” (Dunn Cavelty 2012: 362). In order to achieve this focus, Dunn Cavelty identifies and unpacks three interconnected cybersecurity discourses that she identifies as “technical, cybercrime and cyberespionage, as well as military and civil defence (which highlight fighting wars in the information domain and the need for critical infrastructure protection)” (Dunn Cavelty 2015: 362). Dunn Cavelty explains that information technology terminology is held in the same regard as national security technology such as threats, agents, and vulnerabilities. Finally, she unpacks the hacking tools used by threat agents.

Her article is written reflectively about the forging of cybersecurity and its countermeasures and she adopts a securitisation theory approach to express three cybersecurity discourses and how they have been framed. In doing so, she uses analytical concepts such as threats, agents, and vulnerabilities. The previously mentioned three discourses accompanied by the analytical concepts are used in her cybersecurity adaption of Buzan *et al*. (1998) Securitisation Theory. The key concepts contributing to Dunn Cavelty’s framework are the three discourses previously mentioned, the main actors involved, and the main referent objects according to various discourses. These concepts are used in an adaption of Securitisation Theory. Dunn Cavelty expresses that cybersecurity discourse encompasses information attacks orchestrated by human adversaries using cybertools and the stipulated discourses “encompass threat imaginaries, security practices, referent objects and key actors” (Dunn Cavelty 2015: 365). Dunn Cavelty’s framework informs the framing

of cybersecurity as it proves the notion that multiple cybersecurity discourses coexist, with differing main actors and main referent objects. Furthermore, Dunn Cavelty proposes a second form of analysis that focuses on the countermeasures of each of the three discourses.

Dunn Cavelty's study offers an analytical framework that may be applied to South Africa, in terms of threat framing, Dunn Cavelty raises the point that "the US government shaped both the threat perception and the envisaged countermeasures with only little variation in other countries" (Dunn Cavelty 2012: 364). Thus, Dunn Cavelty's framework offers a foundational basis for further application to test its applicability to a country such as South Africa. Similarly, this framework will assist this study in defining what cybersecurity is in South Africa. Hansen and Nissenbaum's (2009: 1155) seminal work on cybersecurity illustrates the multifaceted grammar of security for the cybersecurity sector, expressing cybersecurity as "hyper-securitisation, everyday security practices and technifications." Dunn Cavelty (2015: 370) similarly illustrates this point through identifying three discourses of cybersecurity which, although identified as different sectors of cybersecurity, are intertwined by nature. Fichtner (2018) provides an updated approach to exploring cybersecurity as constructed within multiple discourses. Cybersecurity is viewed in Fichtner's (2018) article as "a means for data protection, safeguarding financial interests, the protection of public and political infrastructures and as a control of information and communication flows," suggesting that cybersecurity has a diverse set of roles in protecting society.

An assumption that one can identify from the literature on cybersecurity is that it is insecure and, as a result, constantly evolving. It was highly influenced by American politicians and reinforced by American scholars. The concept emerged in the Post-Cold War era and vulnerabilities were projected into cyberspace. Dunn Cavelty clearly expresses that these differing discourses each consist of perceived threats, securitisation of these threats, and objects assumed in need of protection. Despite advances in technology, these referent objects remain relevant.

Dunn Cavelty's framework informs the technical, cybercrime, cyberespionage, and military/civil defence cybersecurity discourses in South Africa by outlining key

concepts for analysis. These concepts are the main actors, referent objects, protection concept, and national and international levels of countermeasures to ensure protection of these cybersecurity discourses. Dunn Cavelty asserts that “the type of malware, the type of targets and the attack vectors all changed with technology and the existing technical countermeasures (and continue to do so).” Further, applying this framework to the context of South Africa’s cybersecurity threat landscape allows for the possibility of new actors, referent objects, and countermeasures at a national and international level. Instead of looking at each cybersecurity discourse separately, this analysis will evaluate and apply these cybersecurity discourses collectively at a national level.

Table one is Dunn Cavelty’s (2015) “Three cybersecurity discourses framework.” This table explains how different cybersecurity discourses are securitised. The main actors involved in the securitisation process and the main referent objects which have been framed to be in need of securitisation measures are indicated. Main actors pertain to the stakeholders involved in the securitisation process. These actors frame security issues within the stipulated cybersecurity discourses. As illustrated in table one, the main actors listed in the technical cybersecurity discourse are computer experts and the anti-virus Industry and the main referent objects are predominately computers and computer networks. Under cybercrime-espionage the main actors are law enforcement and the intelligence community which remain a threat to business networks and classified information networks. The following cybersecurity discourses introduce the national security dimension related to cybersecurity, being identified as military and civil defence. The main actors in this sphere of cybersecurity are national security experts, military, and civil defence. The main referent objects identified in this sphere are military networks, armed forces, and critical information infrastructure. This analytical framework is relevant to the cybersecurity threats section of this study as the technical sector fundamentally covers malware, viruses, worms, and system intrusions. This section conceptualises cybersecurity within a national security context. According to Dunn Cavelty (2015: 370), the “political reading of cybersecurity cannot be divorced from the material realities of computer disruptions and knowledge practices in technical and intelligence communities,” which in turn shape the field constantly through their everyday offensive and defensive behaviour.

3.3.2. Hare

Table two refers to Hare's interpretation of cybersecurity threats according to the analytical concepts of national power and socio-political cohesion. These analytical concepts are ranked according to the degree of national power and socio-political cohesion. Hare's (2010: 1) study pin points "that different national agendas and technology levels amongst the world's states will lead to different prioritisations of cybersecurity threats." Hare's study explores the logic of how countries are driven to prioritise potential cyberattacks differently, based on two determinants, power and social-political cohesion. These analytical factors are applied to the context of cybersecurity within a state and deduce that the degree of the two determinants listed above allows for certain cybersecurity threats to be more prominent in certain countries.

Hare's (2010) article adopts Buzan's (1983) "people, states and fear" categorisation of vulnerability theory to cybersecurity and cyberthreats. However, his study is comparative and addresses two factors that influence certain prioritisations of cyberthreats by various countries. First, he argues that collaborative efforts to create cybernorms cannot be attainable until these vulnerabilities are addressed. Second, Hare (2010: 212) expresses that "cyber-threats can be viewed as national security matters and therefore should be relevant to the Security Studies field and should be analysed using Security Studies theories."

In certain types of states, certain types of cyberthreats are more prominent. The origin of Hare's framework comes from Buzan's vulnerabilities framework which he adapts in order for cyberthreats to be analysed. Hare (2010) modifies Buzan's model to encompass cybersecurity related threats. His study provides relevant international examples with each quadrant of the framework and points out each consequence of various national perceptions on a unified policy formulation aimed at securing cyberspace.

Hare's (2010) framework arose due to an impasse reached at a workshop in 2009 on cybersecurity at the Organisation for Security and Cooperation in Vienna. Hare's focus of his study is aimed at answering the question "why is it difficult to reach a consensus

on the most pressing issue to national security?" (Hare 2010: 1). He explains that this impasse is directly related to two factors: differing national agendas and differing proficiencies regarding technology globally. This, in turn, is the root cause for various states placing higher importance on differing cybersecurity threats. This framework contextualises cybersecurity in national security and articulates "that cyber-threats can be viewed as national security matters and therefore should be relevant to the Security Studies field and should be analysed using Security Studies theories" (Hare 2010: 212). A securitisation and constructivist lens is used in this study to explain both the practice of securitising cyberspace and which stakeholders play an incremental role in ensuring that a cyberthreat is securitised. The framework similarly draws from Buzan (1991).

The units of analysis of this framework are power and social-political cohesion. These concepts are used in this framework to determine the most predominant cybersecurity threats to strong and weak states. Essentially the analytical concepts of Hare's study allow for one to determine what types of threats would be prioritised in a state based on the degree of socio-political cohesion and power in the state. This framework argues that national power and socio-political cohesion play a significant role in characterising and prioritising cybersecurity threats differently. The combination of national power and socio-political cohesion can assess the relative importance of threats from states' perspectives. According to the framework, stronger powers are assumed to have far fewer vulnerabilities and, as a result, it is harder to securitise the security agenda successfully.

Hare's framework investigates how a state might focus on potential digital dangers in an unexpected way. The contention proposed in this article is that contrasting power and socio-political cohesion degrees among the world's states will lead them to focus on network safety dangers in different ways, obstructing endeavours to arrive at an agreement on cyber-related activities. As far as digital dangers go, they might be viewed as security issues and, consequently, their particular defenceless referent items should be securitised. What is obvious from this system is that states have concluded that there is a network safety part to public security (Hare 2010: 216).Hare's primary contention is that digital dangers can be examined according to a viewpoint of safety. The framework introduced surveys of the alternate points of view on network

protection weaknesses dependent on attributes of the state, which was at first introduced by Buzan (1991).

3.4 Value and shortcomings of Hare and Dunn Cavelty's frameworks

Dunn Cavelty's article provides value to this study as she places cyberthreats into perspective. Secondly, she identifies various cybersecurity discourses and illustrates which cybersecurity threats fit into each cybersecurity discourse. Dunn Cavelty further expresses both the actors and referent objects encompassing each cybersecurity discourse and illustrates countermeasures for each discourse. This approach allows for a better understanding of cybersecurity and effectively explains which referent objects would need to be securitised in each discourse. Additionally, Dunn Cavelty's work provides a foundational basis for understanding information security, and it unpacks what information security entails by expressing the deep-rooted insecurity that both computers and networks have. Furthermore, comparing computer security to national security and her expression of similar key concepts in both frameworks allows for an enhanced understanding of what cybersecurity entails.

A shortcoming of the study is that the framework is not applied to a case to test its applicability. A second shortcoming is that cyberthreats have grown both in number and sophistication, and despite Dunn Cavelty's assumption that "cyber-risk is generally overstated" (Dunn Cavelty 2015: 363), rhetoric increasingly suggests the reality behind cyberthreats is fundamentally a logic of those who are aware that they have fallen victim to a hack and those who are unaware of being subject to a hack. Cyberrisk is therefore a genuine concern for all stakeholders in any country.

Although Hare (2010: 221) outlines the advantage of his framework as a manner for "policy makers to understand and reconcile competing policy agendas that result from the securitisation of cyber threats," this framework offers additional valuable information regarding the evident correlation between cybersecurity formulation and cybersecurity agendas. Policy agendas are directly related to the securitisation of cybersecurity threats. Further, this framework proves useful as it can be applied as a tool to evaluate what types of cybersecurity threats are prominent in certain types of

states and it identifies potential ways that different types of states would securitise their cybervulnerabilities.

A shortcoming of this structure is that Hare specifies that this study works best when it is compared to other states. The framework is not intended to characterise a wide range of states completely, nor portray every one of the expected dangers against which a state views itself as defenceless. Further, the analysis is strictly from a state perspective and does not take into consideration various types of cybersecurity threat discourses in one country. A second shortcoming is an absolute measurement of the two concepts of socio-political cohesion and power.

3.6 Conclusion

This chapter focused on evaluating how Dunn Cavelty's 2015 cybersecurity framework informs the framing of cybersecurity. In addition, this chapter located the concept of cybersecurity in theoretical studies. In conclusion, this chapter provides the basis for the next chapter, which focuses on identifying and framing cybersecurity threats. The goal of this chapter was to point out that cybersecurity is multidimensional and, as a result, when one attempts to identify and frame cybersecurity threats, this notion of multi-dimensionality must be acknowledged. Hare and Dunn Cavelty's frameworks complement one another as cybersecurity scholarship forms part of evaluating the nature of the cyberthreat.

The chapter provided guidelines for the identification of cybersecurity threats. The concept of cybersecurity threats was defined as well as explained. As a result, conceptual clarity was expressed between the terms cyberthreats, cybersecurity threats, and cyberattacks. Further, the characterisation of diverse types of cybersecurity threats was illustrated, and a holistic overview was provided of these diverse threats and the threat agents and methods associated with these cybersecurity threats. This chapter expressed how cybersecurity threats are framed by use of theoretical frameworks. In addition, the prominence of certain events which have shaped the perception of cybersecurity threats was expressed. This chapter similarly evaluated Hare's 2010 cybervulnerabilities and types of states framework to determine if the concepts in Hare's framework apply to the study of a country's

cybersecurity and cybersecurity threat landscape. One can deduce that this framework requires an application to a country to examines its effectiveness.

This chapter evaluated Hare's 2010 cybervulnerabilities and types of states framework and Dunn Cavelty's 2015in order to determine if the concepts in Hare's study apply to the study of a country's cybersecurity and cybersecurity threat landscape. Essentially this chapter will guide the identification and framing of cybersecurity threats and the path to understanding a county's cybersecurity threat landscape. The next chapter will explore the cybersecurity threat landscape in South Africa and understand what applying Dunn Cavelty and Hare's frameworks to South Africa entails.

Chapter Four: The identification and framing of cybersecurity threats in South Africa

4.1. Introduction

This chapter will utilise the proposed amended framework illustrated in table 5, to answer how combining Dunn Cavelty and Hare's analytical frameworks informs the identification and framing of cybersecurity threats in South Africa. This chapter will similarly analyse securitisation and threat narratives in South Africa. Additionally, this chapter will discuss how the degree of weakness or strength of South Africa's cyberpower and social-political cohesion on cybersecurity threats, contributes to the framing of certain cybersecurity threats over others. The chapter will answer if in fact South African policymakers conceive of cybersecurity threats as Hare predicts, and if the South African cybersecurity threat discourse is framed according to various discourses identified by Dunn Cavelty.

4.2 Locating Hare and Dunn Cavelty in the context of South Africa

To summarise, Hare's analytical framework expressed in table 4 provides a classification of four groupings of states based on their level of external power and internal social cohesion, and uses this framework to classify state's approaches to cyber politics into four different perspectives. However, in order to maximise the value of utilising this analytical framework's application to South Africa, certain amendments to the analytical framework are necessary. The first change would be to change social-political cohesion to South Africa's social-political cohesion on cybersecurity. Additionally, cyberpower rather than power should be the unit of analysis. The rationale behind these changes is that these units are more relevant measurements than what was initial proposed in 2010 by Hare. Furthermore, these units of analysis guide the analysis of determining what type of state South Africa is classified as and in turn, will identify what types of cybersecurity threats are predominantly evident in the state. The findings from Hare's analysis will allow for further exploration into the framing and identification of cybersecurity threats in South Africa and will evaluate if policymakers in South Africa conceive of cybersecurity threats as Hare predicts. This can be analysed through government documents, speeches, media and bills regarding

cybersecurity threats to determine how cybersecurity threats are framed In South Africa.

4.2.2 South Africa's cyberpower

Cyberpower is argued by Nye (2010 :4) to be "used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace". Nye similarly highlights that cyberpower can further be broken down into soft power or hard power. South Africa's cyberpower will be discussed, and the degree of its strength or weakness will be determined. Additionally, South Africa's cyberpower in relation to cybersecurity threats links to the types of threats identified as cybervulnerabilities in a state.

South African government utilises soft power in cyberspace, which entails utilising information in a strategic manner, to either influence, control the agenda by limiting options or lastly, to frame cybersecurity threats. The reasoning for South Africa utilising soft power rather than hard power is related to South Africa's inability to illustrate the following actions in cyberspace : combat cybersecurity threats through cyberattacks, implementing firewalls and threatening individuals who share censored information. There are two reasons as to why South Africa utilises soft power, over hard power.

South Africa is considered to be a lucrative country for cyberattacks. There are multiple factors contributing to the reason why this is the case. Firstly, South Africa is a democratic country, and as such, cannot limit the civil liabilities of its citizens by censoring cyberspace. Secondly, South Africa's national response to cybersecurity threats correlates with the state's successful "production of cybersecurity professionals" (Biermann & Van der Waag-Cowling 2018). South Africa does not have the national capability to address these cybersecurity threats from a technical perspective as there is a shortage of computer experts/cybersecurity professionals. Unfortunately, South Africa suffers from a shortage of cybersecurity professionals, indicating a cybersecurity skills gap in the country. This is a very real problem related to a country's power in cyberspace, as cybersecurity professionals are able to assist in mitigating or managing cybersecurity threats.

4.3.1 South Africa's social-political cohesion on cybersecurity

In order to measure if South Africa is weak or strong with regards to its socio- political cohesion in relation to cybersecurity threats, an analysis of policy regarding cybersecurity threats in South Africa is necessary. This gives insight into whether or not South Africa manages to implement its policies regarding cybersecurity and whether or not it successfully identifies and frames cybersecurity threats.

The departments and organisations responsible for ensuring cybersecurity in South Africa are: the CSIR, the SITA, the SSA, the SAPS, the Hawks, the SANDF, the Department of Communication and Digital Technologies, and the Department of Defence (which is responsible for the overall co-ordination, accountability, and implementation of cyberdefence measures in South Africa as a core function of its constitutional mandate). Despite efforts made by the SSA in 2012 to stipulate a National Cybersecurity Policy Framework for South Africa, the policy remains more impressive theoretically than in reality. Further "South Africa lags behind when it comes to cybersecurity [and] co-ordination between inter-governmental departments" (PYGMA Consulting 2022).

The Department of Defence's annual report of 2020/2021 identifies the following, "the sad reality is that our equipment is old and becoming older, while the nature of the threats we face are becoming exponentially more technologically advanced, especial in the realm of cybersecurity." Securing cyberspace is not mentioned further in the report and not included as a programme warranting budget structure. This indicates a huge shift from previous efforts in the Department of Defence's annual reports of 2018/2019 (87) and 2019/2020 (15) which specified that South Africa's cyberwarfare strategy had been submitted for approval by the Justice Crime Prevention and Security Cluster minister. The fact that there is no military strategy to secure cyberspace in the Department of Defence's annual report yet Ramaphosa illustrated the necessity of policy regarding cybersecurity threats by signing Act No. 19 of 2020 of the Cybercrimes Act 2020 in 2021, indicates that the South African government has framed cybercrime to be more of cyber threat narrative than cyberwarfare (Phiri 2021).

Furthermore, there is a lack of alignment in policy and strategic vision regarding cybersecurity threats and the South African government is proving reactive rather than proactive. Without a clear vision and sufficient preparedness for unknown cybersecurity threats, South Africa is essentially a sitting duck and an easy target. This fact is rather concerning in light of the cybersecurity threats that South Africa faced in 2021 alone. South Africa has been subject to a number of DDoS attacks and major attacks on its critical infrastructure.

Dunn Cavelty's analytical framework illustrates the various cybersecurity threat discourses and how certain actors frame and identify the how cybersecurity threats are securitised through the use of policy. What is apparent from her study, is that there is no alignment within all the organisations that play a role in cybersecurity in South Africa. The only cybersecurity threat that South African government has attempted to securitise is cybercrime. Dunn Cavelty's cybersecurity threat discourses will be applied to the South African case to explore the framing of various cybersecurity threats by policymakers.

4.2.1 Technical cybersecurity threat discourse in South Africa

In table 3 Dunn Cavelty (2015) illustrates that cybersecurity is broader than just the technical realm of cybersecurity, as a result, various spheres of cybersecurity require securitisation. Further, various policymakers contribute to the framing and identification cybersecurity threats. The technical cybersecurity discourse in South Africa emerged as a result of "a relatively sophisticated Information Communication Technology sector developing in South Africa" (Gillwald *et al*. 2012: 1). This was accompanied by the unprecedented influx in ICT usage, which made "South Africa, like many other countries, dependent on the internet to govern, conduct business and for other social purposes" (RSA DOD 2015: 12).

As expressed in table 3, the main policymakers involved in the framing process of technical cybersecurity discourse are the Centre for Scientific and Industrial Research (CSIR), State Information Technology Agency (SITA) and the anti-virus industry. The CSIR has its own information and cybersecurity research centre and is responsible for building a national cybersecurity structure to respond to cybersecurity threats and

vulnerabilities. The SITA acts as South Africa's "government's IT house of values" (SITA 2022) and plays a significant role in ensuring the availability of e-governance services to all citizens in South Africa. Within these organisations are computer experts dedicated to securing South Africa's cyberspace. The anti-virus industry similarly plays a significant role in identifying cybersecurity threats, picking up cybersecurity trends, and developing software catered to securing information from hackers and malware tools used to wage a cyberattack.

CSIR operates as a decision support function regarding cybersecurity capabilities in South Africa and contributes to the alignment of public and private cybersecurity sectors. The CSIR similarly ensures that both sectors remain in alignment with South Africa's national cybersecurity strategy and therefore the organisation identifies and frames the "approaches to securely identify and protect people (cradle to grave) and systems (physical and digital) against vulnerabilities, threats and risks" (CSIR 2022).

SITA's core function is to act as the harmonious function for South Africa's information technology. Mr, Willie Vukela, Deputy Director General: Government services access and improvement expresses that the South African government wants to "move away from the traditional way of queuing for services" (Gabara 2022). SITA therefore is a pivotal role for the merger between the use of IT for government and citizens in South Africa. On this basis SITA frames the public- private engagement of IT in South Africa.

Anti-virus companies play a significant role in the identification and framing of cybersecurity threats in South Africa, as they publish reports pertaining to cybersecurity threat trends annually. According to Trend Micro's cybersecurity report "South Africa is a playground for cybersecurity criminals, ranking in the top 30 most targeted countries for malware attacks and top 20 for COVID-19 related email threats" (Businesstech 2021). The Anti-virus industry has cybersecurity consultants who evaluate South Africa's cybervulnerabilities, and these individuals play a significant role in the framing of cybersecurity threats and identifying the most prominent cybersecurity threats within a state. Technical experts Accenture (2020) identified the most common types of cyberattacks in South Africa as malware attacks, followed by fraud, android mobile phone hacks, banking malware, and virtual currency related crime. However, there has been a particular increase in phishing and ransomware

attacks. Since the start of the COVID-19 pandemic, phishing attacks have accelerated in South Africa. South Africa currently struggles with spam email traffic as “the number of phishing attacks recorded in South Africa for the first half of 2021 exceeded one million” (Banda 2021). It is also predicted that ransomware will be considered to be one of the top threats for 2022. This type of attack links to cybercrime and its manifestations will be further discussed in the cybercrime and cyberespionage discourse.

The main referent objects identified in need of information assurance in this discourse are computers/computer networks, electronic devices, and social networks. The cybersecurity hub operates as South Africa’s National Computer Security Incident Response Team (CSIRT), which falls under the realm of the Department of Telecommunications and Postal Services. The State Security Agency is the South African government’s CSIRT and South African National Research Network (SANRen) is a CSIRT for public universities and academics. The cybersecurity hub identifies and frames cybersecurity threats through the cybersecurity awareness information that the organisation generates and distributes to South African citizens. Whereas the SANRen is responsible for “preventing and responding to IT security incidents” (SANRen CSIRT 2022). SANRen further conducts vulnerability assessments, which assist in the identification and framing of cybersecurity threats in South Africa. On an international level South Africa is mandated to comply with international information security standards.

4.2.2 Cybercrime threat discourse

Dunn Cavelty combines cybercrime and cyberespionage in her framework. However, it is evident in South Africa that cybercrime and cyberespionage are very much two separate discourses. Therefore, these cybersecurity threats will be will assessed separately in the context of South Africa. Cybercrime is defined according to the RSA DOD (2015: 2-18) as “involving, inter alia, malware, viruses, identity theft, intentional and unauthorised access, modification to and interception of computer data or programmes, computer-related extortion, fraud and forgery.” According to Dunn Cavelty’s framework, law enforcement and the intelligence community are responsible for the framing of the cybercrime and cyberespionage discourse. In the context of

South Africa, this is translated to the South African Police Service (SAPS), the State Security Agency (SSA), and the Hawks (the South African Police Services' Directorate for Priority Crime Investigations). These actors are responsible for protecting the business sector and classified information in South Africa.

Dlamini and Modise (2012: 22) expressed that cybercrime was a very serious concern in South Africa, as it threatened South Africa's national security already in 2012. To this end, the cybercrime discourse has received more attention than other cybersecurity threats in South Africa. The South African government has framed cybercrime to be the most prominent cybersecurity threat in South Africa. To epitomise this, South Africa's recent Cybercrimes Act is an indication of concern surrounding cybersecurity threats. President Cyril Ramaphosa recently made it clear that defence against cybercrime is imperative. This is evident through Ramaphosa signing the Cybercrimes Bill. This bill places South Africa's cybersecurity laws in line with the rest of the world and indicates a commitment to defending South Africa and its citizens against cybercrime. This cybercrime bill recognises the SAPS as the main office to facilitate investigations and it currently should be satisfactorily capacitated to do as such. Execution requires the offices of SAPS, private partners, and digital specialists to cooperate. In spite of huge execution challenges, the new bill flags the country's obligation to worldwide digital security (Allen 2021) and brings South Africa up to international standard for fighting cybercrime.

This is partially due to South Africa being a lucrative target. The COVID-19 pandemic placed extra pressure on the state, as various sectors of South Africa's economy were forced to work from home and rely more on ICT. Statistically, according to a TransUnion Survey, "42% of South African households have been targeted by COVID-19 related scams, an increase of 14% since the lockdown started in April last year" (Tshal 2021), justifying the need for policy on cybercrime. Although initiatives exist which help raise awareness regarding cybersecurity and cybersecurity threats in South Africa, a large portion of the population still fall victim to cybercrime without even realising it. The shift towards citizens using the internet to conduct their everyday life, such as online banking, online South African Revenue Service (SARS) applications, as well as using mobile devices, places citizens at risk of falling victim to cybercrime. Furthermore, many South African businesses have also fallen victim to denial of

service (DoS) and ransomware attacks. In fact, in South Africa the most common type of method used to wage an attack is ransomware (Lotz 2021).

Cyberespionage threat discourse

Cyberespionage framed as a concern to the state on both a corporate and national level, by the State Security Agency and the Hawks. However, the State Security Agency is subject to corruption which influences its ability to successfully frame any cybersecurity threat, this is due to the fact that in order for something to be securitised citizens need to agree that the issue is security issue and therefore need to be convinced by the State Agency of the threat. Cyberespionage is however identified in a South African context by South African Defence Review (2015: 2-18) as “the silent gathering of classified information without the permission of the holder of the information.” Referent objects of this sphere of cybersecurity within South Africa are business networks, classified information and government networks. The protection measure for information assurance on a national level is computer law and on an international level is ensuring that South Africa complies with conventions on cybercrime. Furthermore, mutual jurisdiction assistance procedures are required in order to ensure information assurance

A manifestation of this type of attack occurred when South Africa’s SSA spy cables were leaked by Al Jazeera in 2015. These leaks compromised national security as they divulged “security flaws and lapses within South African government and intelligence services” (Van Heerden *et al*. 2016: 7). The SSA’s role is to determine potential security concerns in South Africa, yet it was subject to an astronomical security breach itself.

In July 2021 South Africa’s state-owned enterprise Transnet was subject to a cyberattack that disrupted cargo movement and, most importantly, trading routes. According to Reva (2021), what makes this cyberattack noteworthy is that “for the first time the operational integrity of the country’s critical maritime infrastructure … suffered a severe disruption.” This disruption impacted the political sector of the country as it undermined a R100 billion commitment Ramaphosa had made in May 2021 to infrastructure development with the goal of making Durban South Africa’s best

functioning port. As per Allen's (2021) observation, "for developing countries such as South Africa cyberattacks on critical national infrastructures are potentially devastating." The cyberattack on Transnet pointed out exactly how vulnerable South Africa is to a cyberattack on a state-owned enterprise. Most importantly, as this attack focused on disrupting the state's critical national infrastructure, it was escalated to a matter of national security. Additionally, in 2021 cyberattacks on both the South African Space Agency and the Department of Justice occurred. These cyberattacks raise great concern as ransomware was applied in order to wage these attacks on both organisations which are intrinsic to South Africa (Toyana 2021). These types of attacks on such critical organisations imply that cybercrime – although important – is not the only cybersecurity threat worth securitising.

4.2.3 Military/civil defence discourse

The transformation of our communication environment has played an incremental role in the transcendence of politics to the digital sphere and topics such as cybersecurity and cybersecurity threats have made their way into political discussions globally. This is no different in the case of cybersecurity and cybersecurity threats in South Africa as technology has enabled new ways of pursuing political ends, even in democratic countries like South Africa. Cybersecurity is increasingly important in shaping a state's national interest and, in turn, makes these states vulnerable to attacks as a result of politics migrating online. Cyberspace is recognised globally as a "fifth dimension of conflict" (Martino 2021). Because an idealised vision of cyberspace has been promoted, the information society has become an arena for political agenda. However, cybersecurity threats remain problematic on account of a few complexities. Firstly, the differentiation between the 'real' and 'cyber' world have become incredibly complex to separate and the line between war and peace is not clear. Therefore, countries globally need to automatically assume that they are constantly under attack to ensure that their cybersecurity remains as up to date as possible. Secondly, the ratio between cyberattacks and cybersecurity is not equal. Cyberattacks advance more rapidly and cybersecurity technicians and national cybersecurity experts are unable to keep up. South Africa already has an astronomical shortage of cybersecurity technicians, which makes it even more vulnerable to cyberattacks.

This cybersecurity discourse pertains to the securing of South Africa from threats such as cyberwarfare and cyberterrorism. The Department of Defence is responsible for the defence against cyberattacks on South Africa's infrastructure and defence facilities (RSA Parliament 2020: 2). The DOD is mandated to secure cyberspace, and to ensure that all people in South Africa are and feel safe as pertaining to digital or physical threats. There is a clear nexus between the political sphere and the military/civil defence of South Africa as political issues directly affect the nature of cyberthreats seen in a country. Organisations such as the South African National Defence Force (SANDF), the Armaments Corporation of South Africa (ARMSCOR), Department of Communication and Digital Technology and the Department of Defence are the actors involved in the framing military/ civil cybersecurity discourse. The main referent objects are military networks, networked forces, and critical infrastructure. Information assurance remains central to the securitisation of this discourse.

The South African government has placed cybersecurity as a priority on the county's national security agenda (Molwantwa 2019: 1). The military/civil defence sphere of cybersecurity has gained much attention in South Africa and a number of cybersecurity measures can be seen as the "securitization of cyberspace" by the South African government (Molwantwa 2019: 1). The South African government's rhetoric and mass media surrounding cyberspace, cybersecurity, and cyberthreats are a manner in which to assess these concepts. This, in turn, illustrates the framing of a concept/phenomena through the use of speech acts and media. Various speech acts and actions domestically and internationally help us evaluate the position that South Africa takes on cybersecurity and cybersecurity threats.

It is important to express South Africa's position in cybersecurity discussions in international organisations. Cybersecurity and cybersecurity threats cannot be viewed in isolation as cyberspace holds no borders. No country is immune to cybersecurity threats and therefore platforms such as the African Union and United Nations are important when identifying global/regional cybersecurity norms. The lack of global cybersecurity norms, despite international efforts by respected organisations such as the United Nations and the African Union, contributes to heightened uncertainty regarding cyberattacks and possible cyberthreats.

South Africa is a state which has an influx of cybersecurity threats but that lacks the capability to address these cybersecurity threats from a technical perspective as it has a shortage of skilled computer experts/cybersecurity professionals. This is a huge concern, not only at a national level, but for corporates and individuals alike. In lieu of this fact, South Africa government began concerted efforts to ensure national cybersecurity awareness in the country and frames cybersecurity to be the combined responsibility of civil society, government, and the private sector. The management of the above-mentioned cybersecurity threats which exist within the cybersecurity discourses remains a problem as, according to Biermann *et al*. (2018), “South Africa, like most countries, is failing to produce enough cybersecurity specialists to secure its digital space.” As illustrated by Dunn Cavelty, at a national level these professionals are required to play a significant role in the assurance of information by implementing a Computer Security Incident Response Team (CSIRT). The required skill set is fundamental to the securing of computers and computer network security as well as all electronic devices connected to a network. Cybersecurity has only gained attention in recent years, as it was not a sought-after profession in South Africa initially, especially as much of the population in rural communities was not technologically proficient. More recently, the lack of technical experts in South Africa has made South Africa increasingly reliant on foreign cybersecurity professionals. In turn, the use of foreign software/hardware makes the state incredibly vulnerable to cybersecurity threats.

According to a World Economic Forum article written by Masterson (2021), despite a lack of technical experts in cybersecurity, solutions are being sought which aim to close “the cybersecurity skills gap in South Africa, where marginalized youth are training at academies in Cape Town and Johannesburg.” Absa bank is championing this initiative, which allows for at risk youth to become involved in skills development instead of drugs, alcohol, and crime. There are free cybersecurity learning platforms such as Trailblazer which make available free courses which focus on training cybersecurity professionals. Despite these courses which are freely available, a massive inequality gap is apparent in South Africa as not all South Africans have the means to afford Wi-Fi or internet to access these free courses.

Framing constitutes the construction of phenomena, and is executed through the use of media and political rhetoric. This in turn shapes perceptions of the phenomena. In the case of cybersecurity, “while the common topic in all communities is the security of computers and computer networks, they differ most in their focus on the types of issues on a higher level, which they regard as being connected to or influenced by the security of computers and computer networks” (Dunn Cavelty 2015: 108). Therefore, placing different referent objects in different contexts allows for the shaping and driving of discourses surrounding cybersecurity threats.

3.5 Synthesis of Dunn Cavelty and Hare’s frameworks

Combining the analytical concepts from both frameworks is important to this study as applying these concepts concurrently to the context of South Africa, allows for a deeper analysis of the framing of cybersecurity threat discourses. Additionally, it allows exploratory research regarding if SA policy makers illustrated in Dunn Cavelty’s analytical framework do infact frame cybersecurity threats in South Africa as “technical threats, cybercrime- cyberespionage, military/ civil defence”. Furthermore, combing the analytical frameworks allows for deeper analysis into if policymakers in South Africa conceive of cybersecurity threats as Hare predicts. Although, Dunn Cavelty and Hare’s analytical frameworks provide a sound foundation for exploring cybersecurity threats in South Africa. Table four illustrates the adapted framework.

Further it is evident in South Africa that cybercrime and cyberespionage are viewed as two separate cybersecurity threats, as opposed to what is expressed by Dunn Cavelty. As securitisation is central to this study, the ability for a policy maker to securitise a cybersecurity threat based on the types of attacks that are framed as cybersecurity threats is an indication as to what threat narratives exist . The above allows for analysis regarding if a state is weak or strong in relation to cybersecurity threats. The cybersecurity discourses mentioned by Dunn Cavelty are included in this analytical framework as they encompass actors, referent objects. This analytical framework allows for the exploration into if SA policy makers infact conceive of cybersecurity threats primarily in terms of proposed cybervulnerabilities by Hare ? Table four illustrates the adapted framework.

4.4 Conclusion

As a result of navigating the most prominent cybersecurity threats in South Africa the amended analytical framework paves a path to the second question to be answered in this study – how Cavelty's analytical framework informs the framing of cybersecurity threats in South Africa. Dunn Cavelty's analytical framework focuses on the social construction of "cybersecurity threat" discourses. Locating Cavelty's analytical framework as illustrated in table 3, into the context of South Africa is equally as important as illustrated with Hare's analytical framework earlier , as it allows for one to evaluate what type of cybersecurity threat discourse is most prominent in South Africa, as well as ague that cybersecurity threats in South Africa are framed according to a certain cybersecurity threat discourse by policymakers in order to securitise main referent objects associated to certain cybersecurity threat discourse.

In conclusion, the application and combination of Dunn Cavelty and Hare's frameworks allowed for a clearer understanding of the framing and Identification of cybersecurity threats in South Africa. Dunn Cavelty's framework provided the necessary analysis required to apply the evaluation of South Africa's socio-political cohesion on cybersecurity threats and cyberpower. Although the objective of the study is to apply Hare and Dunn Cavelty's frameworks analytically, there was most certainly value to adapting both frameworks to the South African context before utilising the frameworks to answer the research question of the study. South Africa's cybersecurity and cyberthreat landscape is complex and multi-dimensional. This chapter's objective was to apply Dunn Cavelty and Hare's frameworks to the South African cybersecurity landscape in order to understand, describe, and explore the way in which South Africa identifies certain cybersecurity discourses and the cybersecurity threats that they constitute. It is essential to acknowledge that the manner in which cybersecurity threats are framed is proportionately related to the type of state as illustrated by Hare (2010).

5. Chapter Five: Findings and conclusion

5.1 Introduction

This final chapter consists of the findings, recommendations, and concluding remarks of this study. The overarching aim of this study was to understand the identification and framing of cybersecurity threats in South Africa through the application of Dunn Cavelty and Hare's frameworks to South Africa. This study addressed the research problem of a gap in the literature on the identification and framing of cybersecurity threats in South Africa. In addition, this study answered the following research question: "How does combining Dunn Cavelty and Hare's framework inform the identification and framing of cybersecurity threats in South Africa?" and bridged the gap between a humanities conceptualisation of cybersecurity threats and technical threats.

This study addressed what cybersecurity discourse threats emerge, what their characteristics are, and how South Africa may prioritise specific cybersecurity threats, based on the determinants such as cyberpower and social-political cohesion on cybersecurity threats. The overarching aim of the study was achieved through understanding the framing of cybersecurity in South Africa and the identification and framing of cybersecurity threats in South Africa by utilising concepts from Dunn Cavelty (2015) and Hare's (2010) analytical frameworks and applying these frameworks to South Africa.

Too often cybersecurity is expressed merely in a technical manner which creates confusion for people who are not cyber proficient. This study in turn, provided comprehensive insight into cybersecurity threats, and understanding how they are framed in South Africa.

5.2. Findings

In this section I present the findings from the analysis conducted in the previous chapter. This study sought to answer the research question "How does combining Dunn Cavelty's and Hare's framework inform the identification and framing of cybersecurity threats in South Africa?"

Three findings are made in this study. The first finding is that Dunn Cavelty and Hare's frameworks can, in fact, be applied successfully to South Africa. What can be deduced from the study is that cybersecurity threats can fall into the technical, cybercrime-cyberespionage, or military/civil cybersecurity discourse of a country. Further, in the case of South Africa, cybersecurity threats are identified and framed by main actors within the three cybersecurity discourses. What is apparent from the combination of these two frameworks is that cybersecurity policy identifies cybercrime threats as the most prominent cybersecurity threat in South Africa in need of securitising. The second finding is that South Africa has limited cyber capability due to underfunding and since 2012 has had reduced expenditure for developing a cyberwarfare strategy. This indicated that the South African government and defence capabilities do not identify or frame cyberwarfare as a prominent cybersecurity threat in South Africa. The third finding – and a central problem – is that South Africa suffers from a shortage of cybersecurity professionals.

Firstly, Dunn Cavelty and Hare's frameworks guide the study by analysing cybersecurity threat narratives in South Africa. To be more precise, how policymakers in South Africa frame cybersecurity threats as certain type of cybersecurity threat discourse. Additionally, the analytical framework allowed for analysis regarding what type of state South Africa is categorises as according to Hare's typology. This classification is significant, as the type of state is directly proportionate to the state's cyberpower and social-political cohesion on cybersecurity threats. South Africa was classified as weak on both accounts of cyberpower and social-political cohesion on cybersecurity threats. Policymakers in South Africa conceive of cybersecurity threats in terms of "destabilising political actions in cyberspace, attacks on internet, infrastructure, criminal activities" as predicted by Hare.

Additionally, South Africa has clearly has prioritised the securitisation of cybercrime despite other apparent cybersecurity attacks within the state. The analysis above suggests that in South Africa cybersecurity threats are framed as cybercrime threats to business networks. Therefore, this study finds that cybersecurity threats in South Africa are framed as "cybercrime" threats to business networks as this type of threat is articulated as the most prominent cybersecurity threat in need of securitisation through policies.

In respect to theoretical application, Hare and Dunn Cavelty's frameworks encapsulated South Africa's cybersecurity threat landscape successfully. This is illustrated through the use of tables in which analytical concepts from both scholars are adapted to a South African context. South Africa has multiple cybersecurity discourses which various stakeholders/actors determine and different referent objects which need to be secured from cybersecurity attacks. Similarly, South Africa's ranking of weak socio-political cohesion on cybersecurity and weak cyberpower in cyberspace indicates that the state needs to invest in the training of more cybersecurity professionals internally to manage this threat.

Conclusion

In conclusion, this study contributes to furthering the knowledge of cybersecurity and cybersecurity threats in South Africa by not only describing cybersecurity framing in South Africa, but similarly, identifying the cybersecurity threats in South Africa. The reason why the cybersecurity skills gap is problematic is due to the fact that South Africa has a high cybercrime rate. Phishing and ransomware are the most popular forms of cybersecurity attack tools used in South Africa. South Africa has also suffered from attacks on its critical national infrastructure which is concerning for two reasons. If vulnerabilities are present and not protected in future, these vulnerabilities will become gateways for hackers. Further, if critical state infrastructure is not sufficiently secured in a developing country, the country will not be able to economically recover from a massive cyberattack.

Although South Africa has made a concerted effort to implement acts and bills targeted towards managing cybersecurity threats, without the correct expertise and a correlation between practical measures put in place to secure the state, cybersecurity threats will continue to advance and eventually South Africa will not be able to protect its infrastructure without intervention from cybersecurity specialists in foreign countries.

5.3 Future studies

The findings in this study postulate that Dunn Cavelty and Hare's framework can infact be applied to the South African case study, in order to understand the identification and framing of cybersecurity threats in South Africa. This study opens up opportunity for future research that will help inform Security Studies knowledge on cybersecurity threats could use Hare's framework to compare South Africa's cybervulnerabilities with other states. Additionally, research into global events that shaped South Africa's perception of cybersecurity threats would similarly be a useful study that may offer valuable insight into the framing of cybersecurity threats in South Africa. Lastly, research into South Africa's cybercapability in the case of an attack on its critical infrastructure would be beneficial.

Bibliography

Accenture. 2020. Insight into the cyber threat landscape in South Africa. Internet: https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa. Access: 20 September 2021.

Allen, K. 2021. South Africa lays down the law on cybercrime. Internet: https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime. Access: 15 September 2021.

Banda, M. 2021. Kaspersky records over two million phishing attacks in South Africa, Kenya and Nigeria in H1 2021. Internet: https://www.intelligentcio.com/africa/2021/09/14/kaspersky-records-over-two-million-phishing-attacks-in-south-africa-kenya-and-nigeria-in-h1-2021/#. Access: 22 September 2021.

Bay, M. 2016. What is cybersecurity? In search of an encompassing definition for the post-Snowden era. French Journal for Media Research, 6: 1-23.

Baylis, J., Wirtz, J. J. & Gray, C. S.2010. Strategy in the Contemporary World. Oxford University Press Publisher.

Biermann, E. & Van der Waag-Cowling, N. 2018. Mind the Gap: Addressing South Africa's cybersecurity skills shortage. Internet: https://www.dailymaverick.co.za/article/2018-07-13-mind-the-gap-addressing-south-africas-cybersecurity-skills-shortage/. Access: 20 February 2022.

Brangetto, P. & Veenendaal, M. 2016. Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. Internet: https://www.researchgate.net/publication/305871769_Influence_Cyber_Operations_The_use_of_cyberattacks_in_support_of_Influence_Operations. Access: 20 March 2021.

Buzan, B. 1991. People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era. Brighton: Wheatshef Books.

Buzan, B., Wæver, O. & De Wilde, J. 1998. Security: A New Framework for Analysis. Colorado: Lynne Rienner Publishers.

Canadian Centre for Cybersecurity. 2021. An Introduction to the Cyber Threat Environment. Internet: https://cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf. Access: 8 February 2021.

Carr, J. 2011. Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media,Inc.

Ciolan, I. M. 2014. Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. Revista de Administratie Publica si Politici Sociale, 12 (1) : 40.

Cornish, P., Livingstone, D., Clemente, D. & Yorke, C. 2021. On Cyber Warfare: A Chatham House Report. Internet: https://www.academia.edu/1242693/On_Cyber_Warfare. Access: 19 April 2020.

Craigen, D., Diakun-Thibault, N. & Purse, R. 2014. Defining cybersecurity. Technology Innovation Management Review, 4 (10): 13-21

CSIR. 2022. Defence and Security. Internet: https://www.csir.co.za/defence-and-security. Access: 22 February 2022.

RSA Parliament. 2020. Cyber Security and the South African National Defence Force. Internet: https://static.pmg.org.za/200311CYBER_SECURITY.pdf Access: 1 March 2022.

Dlamini, Z. & Modise, M. 2012. Cyber security awareness initiatives in South Africa: A synergy approach. Internet: https://www.semanticscholar.org/paper/Cyber-security-

awareness-initiatives-in-South-a-Dlamini-Modise/2b9a343c4fe907a71cf34c6df7470389b85efdbe.Access: 19 September 2021.

Dunn Cavelty, M. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cybersecurity Discourse. International Studies Review,15 (1): 105-122.

Dunn Cavelty, M. 2014 .Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Sci Eng Ethics, 20: 701–715.

Dunn Cavelty, M. 2015. Cyber-Security. In Contemporary Security Studies, edited by Collins, A. 3rd Edition. Oxford: Oxford University Press.

Eriksson, J. & Giacomello, G. 2006. The Information Revolution, Security and International Relations: (IR)relevant Theory? International Political Science Review, 27 (3): 221–244.

Fichtner, L. 2018. What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, 7 (2).

Forcepoint. 2020. What is Cybersecurity? Cybersecurity defined, explained, and explored. Internet: https://www.forcepoint.com/cyber-edu/cybersecurity. Access: 7 July 2020.

Futter, A. 2018. 'Cyber' semantics: why we should retire the latest buzzword in security studies. Journal of Cyber Policy, 3 (2): 201-216.

Gabara, N. 2022. DPSA's DDG Vukela appointed to new SITA Board. Internet: https://www.dpsa.gov.za/thepublicservant/2022/02/03/dpsas-ddg-vukela-appointed-to-new-sita-board/. Access: 1 March 2022.

Galinec, D., Možnik, D. & Guberina, B. 2017. Cybersecurity and cyber defence: national level strategic approach. Automatika: Journal for Control, Measurement, Electronics, Computing and Communications, 58 (3): 273-286.

Gamero-Garrido, A. 2014. Cyber Conflicts in International Relations: Framework and Case Studies. Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427993. Access: 24 April 2021.

Gillwald, A., Moyo, M. & Stork, C. 2012. Understanding what is Happening in ICT in South Africa: A Supply-and Demand-side Analysis of the ICT Sector. Internet: https://www.africaportal.org/publications/understanding-what-happening-ict-south-africa-supply-and-demand-side-analysis-ict-sector/.Access: 01 March 2022

Grant, J. & Booth, A. 2009. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Information and Libraries Journal, 26 (2): 91-108.

Griffiths, J. L. 2017. Cyber security as an emerging challenge to South African national security. Pretoria: University of Pretoria.

Hansen, L. & Nissenbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53 (4): 1155-1175.

Hare, F. 2010. The Cyber Threat to National Security: Why Can't We Agree? In Conference on cyber conflict proceedings, edited by C. Czosseck & K. Podins. Tallinn: CCD COE Publications.

Herzog, S. 2011. Revisiting the Estonian cyber-attacks: Digital threats and multinational responses. Journal of Strategic Security, 4 (2), 49-60.

Israel, I. & Tabansky, L. 2011. An Interdisciplinary Look at Security Challenges in the Information Age. Military and Strategic Affairs, (3) 3: 21-37.

Jabbour, K. & Devendorf, E. 2017. Cyber Threat Characterization. Internet: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Cyber%20Threat%20Characterization_Jabbour_Devendorf.pdf?ver=2018-07-31-093724-720. Access: 13 November 2020.

Jahankhani, H., Al-Nemrat, A. & Hosseinian-Far, A. 2014. Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhgar, A. Staniforth & F. Bosco. Waltham: Syngress.

Jarmon, J. A. & Yannakogeorgos, P. 2018. The Cyber Threat and Globalization: The Impact on US National and International Security. Journal of Strategic Security. San Jose.Rowman & Littlefield.(11) (4) 85-88.

Jefferson, B. 2021. The 15 Most Common Types of Cyber Attacks. Internet: https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/. Access: 8 June 2021.

Lewis, J. A. 2002. Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: Center for Strategic & International Studies.

Lewis, J. A., 2014. National perceptions of cyber threats. Strategic Analysis, 38 (4): 566-576.

Libicki, M. 2009. Cyberdeterrence and Cyberwar. Internet: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf. Access: 25 May 2020.

Libicki, M. 2016. Is There a Cybersecurity Dilemma? The Cyber Defense Review, 1 (1): 129-140.

Liebetrau, T. & Christensen, K. 2020. The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. European Journal of International Security, 6 (1): 1-19.

Lotz, Brendyn. 2021. South Africa has more cybercrime than you realise. Internet: https://www.htxt.co.za/2021/10/south-africa-has-more-cybercrime-than-you-realise/. Access: 21 February 2022.

Madžarević, V. 2016 .Political Regime Matters? Framing the Speech Act in Securitization Of Cyberspace in The USA And China. Masters thesis, Central European University, Hungary.

Maness, R. C. & Valeriano, B. 2016. The impact of cyber conflict on international interactions. Armed Forces & Society, 42 (2): 301-323.

Marsili, M. 2019. The war on cyber terrorism. Democracy and security, 15 (2): 172-199.

Martino, Luigi. 2021. Can Cyberspace Be Governed? Internet: https://www.ispionline.it/en/pubblicazione/can-cyberspace-be-governed-31540. Access: 26 February 2022.

Masterson, V. 2021. This cybersecurity academy is changing lives in South Africa. Internet: https://www.weforum.org/agenda/2021/05/africa-absa-cybersecurity-academy-skills-shortage/. Access: 19 September 2021.

Matthews, D., Arta, H. & Hale, B. 2016. Cyber Situational Awareness. The Cyber Defense Review, 1 (1): 35-46.

Molwantwa, D. M. 2019. Aligning the constitutional rights of citizens with cybersecurity measures in South Africa. Masters thesis, North-West University, South Africa.

Mutimer, D., Grayson, K. & Beier, J. M. 2013. Critical studies on security: An introduction. Critical Studies on Security, 1 (1): 1-12.

Mutune, G. 2021. The Quick and Dirty History of Cybersecurity. Internet: https://cyberexperts.com/history-of-cybersecurity/. Access: 18 September 2021].

National Institute of Standards and Technology. 2021. Glossary: Cyber Threat. Internet: https://csrc.nist.gov/glossary/term/threat. Access: 06 February 2022.

Nissenbaum, H. 2005. Where Computer Security Meets National Security. Ethics and Information Technology, 7 (2): 61-73.

Nye, J. S. 2010. Cyber power. Internet: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. Access: 25 November 2019.

Nyman, J. 2018. Securitization. In Security Studies, United Kingdom: Routledge:100-113.

Olivares, M. 2018. Has Critical Security Studies Run Out of Steam? E-International Relations. Internet: https://www.e-ir.info/2018/05/02/has-critical-security-studies-run-out-of-steam/. Access: 10 October 2020.

Panda Security. 2021. What is Hacktivism? Campaigns That Shaped the Movement. Internet: https://www.pandasecurity.com/en/mediacenter/technology/what-is-hacktivism. Access: 13 July 2021.

Pandey, K. K. & Punia, D. K. 2014. Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. Energy policy, 65: 126-133.

Payne, B. K. 2020. Defining Cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance, edited by T. Holt & A. Bossler. Cham: Palgrave Macmillan.

Phiri, C. 2021. Minister Ronald Lamola welcomes the coming into operation of certain sections of the Cybercrimes Act. Internet: https://www.justice.gov.za/m_statements/2021/20211201-ms-CybercrimesAct_Min.html. Access: 11 February 2022.

PYGMA Consulting. 2022. Cybersecurity Governance In South Africa: A Perspective On Policy, Legislation And Regulation. Internet: https://pygmaconsulting.com/cybersecurity-governance-in-south-africa-a-perspective-on-policy-legislation-and-regulation/. Access: 18 February 2022.

Republic of South Africa (RSA). 2015. Department of Defence (DOD) Review. Cape Town: DOD.

Republic of South Africa (RSA). 2019 Department of Defence (DOD) Annual Report 2018/2019. Cape Town :DOD.

Republic of South Africa (RSA).2020. of Department Defence (DOD) Annual Report 2019/2020. Cape Town: DOD.

Republic of South Africa (RSA). 2021 Department of Defence (DOD), Annual Report 2020/2021. Cape Town :DOD.

Reva, D. 2021. Cyber-attacks expose the vulnerability of South Africa's ports. Internet: https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports. Access: 01 March 2022.

Reveron, D. 2012. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, D.C.: Georgetown University Press.

SANRen CSIRT. 2022. The South African National Research Network: Computer Security Incident Response Team. Internet: https://csirt.sanren.ac.za/. Access: 1 March 2022.

Shipley, T. G. & Bowker, A. 2014. Internet Criminals. In Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace, edited by T. G. Shipley & A. Bowker. Waltham: Syngress.

Siboni, G. 2013. Cyberspace and National Security: Selected Articles. Tel Aviv: Institute for National Security Studies.

Singer, P. & Friedman, A. 2013. Cybersecurity and Cyberwar: What Everyone Needs To Know. New York: Oxford University Press.

SITA. 2022. About SITA. Internet: https://www.sita.co.za/page/about. Access: 12 February 2022.

Smith, T. E. 2013. Cyber warfare: A misrepresentation of the true cyber threat. American Intelligence Journal, 31 (1): 82-85.

Snyder, C. A. 2012. Contemporary security and strategy. In Contemporary security and strategy, edited by Snyder, C. A. Hampshire: Palgrave Macmillan.

Stevens, T. 2018. Global cybersecurity: new directions in theory and methods. Politics and Governance, 6 (2): 1-4.

Talihärm, A. M. 2010. Cyberterrorism: In Theory or in Practice? Defence Against Terrorism Review, 3 (2): 59-74.

Tatar, U., Karabacak, B. & Gheorghe, A. 2016. Internet: https://fuse.franklin.edu/facstaff-pub/37/. Access: 24 April 2020.

Tikk, E. 2011. Ten rules for cybersecurity. Survival, 53 (3): 119-132.

Toyana, M. 2021. Internet: https://www.dailymaverick.co.za/article/2021-09-09-cyber-bandits-target-south-africa-department-of-justice-space-agency-hit-by-ransomware-attacks. Access: 24 September 2021.

Tshal, A. 2021. Cybersecurity Trends To Watch In 2021. Internet: https://www.techfinancials.co.za/2021/01/18/cybersecurity-trends-to-watch-in-2021/. Access: 11 August 2021.

Ulum, M. 2017. Literature Review on Cybersecurity Discourse. Internet: https://www.researchgate.net/publication/324413927_Literature_Review_on_Cyber_Security_Discourse. Access: 1 March 2022.

United States Office of the Director of National Intelligence. 2019. National Intelligence Strategy of the United States of America. Internet:

https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf. Access: 20 June 2020.

Van Heerden, R., Von Som, S. & Mooi, R. 2016. Classification of Cyber Attacks in South Africa. Internet: Available from: https://researchspace.csir.co.za/dspace/handle/10204/8930. Access: 29 March 2021.

Walt, S .M. 1991. The renaissance of security studies. International studies quarterly, 35 (2): 211-239.

Weimann, G. 2004. Cyberterrorism: How real is the threat? Internet: https://www.usip.org/sites/default/files/sr119.pdf. Access: 10 March 2021.

White, J. 2016. Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. Global Security Studies, 7 (4).

Williams, P. D. & McDonald, M. 2018. An introduction to security studies. In Security Studies, Routledge.

Appendix

Table 1: Dunn Cavelty's three cybersecurity discourses framework

	Technical	Crime-espionage	Military/civil defence
Main Actors	• Computer experts • Anti-virus industry	• Law enforcement • Intelligence community	• National security experts • Military • Civil defence establishment
Main Referent Object	• Computers • Computer networks	• Business networks • Classified information (government networks)	• Military networks, networked armed forces • Critical information infrastructure
Protection Concepts	Information assurance		
National Level	• CERTS (specific for different domain, milCert, govCert, etc) • International information security standards	• Harmonisation of law (conventions on cybercrime)	• Arms control • International behavioural norms

Source: Dunn Cavelty (2015: 374)

Table 2: Hare's cybervulnerabilities

		Socio-political cohesion	
		Weak	Strong
National power	Weak	Destabilising political actions in cyberspace, attacks on internet, infrastructure, criminal activities	DDoS and other major attacks on critical infrastructure
	Strong	De-stabilising political actions in cyberspace	Criminal activities in cyberspace

Source: Hare (2010: 218)

Table 3: Dunn Cavelty's framework adapted to South Africa

	Technical	**Cybercrime-cyberespionage**	**Military/civil defence**
Main actors	CSIR SITA Anti-virus industries	SAPS SSA Hawks	ARMSCOR SANDF Department of Communication and Digital Technology Department of Defence
Main referent objects	Computers/computer networks All electronic devices connected to the internet Social networks	Business networks Classified information/government networks	Military networks, networked forces Critical infrastructure
Protection concept	Information assurance		
National level	Cybersecurity Hub (South Africa's National CSIRT) Specific for different government domain, milCert, govCert, etc	Computer law	Critical information infrastructure protection Resilience Cyberoffence, cyberdefence, cyberdeterrence

Table 4 : Hare Applied to South Africa

		South Africa's social-political cohesion on cybersecurity threats	
		Weak	Strong
South Africa's Cyberpower	Weak	Destabilising political actions in cyberspace, attacks on internet, infrastructure, criminal activities	DDoS and other major attacks on critical infrastructure
	Strong	Destabilising political actions in cyberspace	Criminal activities in cyberspace

Table 5 :Amended proposed analytical framework

			South Africa's social-political cohesion on cybersecurity threats			
			Technical	**Cybercrime**	**Cyberespionage**	**Military-Civil**
			Weak		Strong	
South Africa's Cyberpower	**Securitise Security issues**	Weak	Destabilising political actions in cyberspace, attacks on internet, infrastructure, criminal activities		DDoS and other major attacks on critical infrastructure	
		Strong	Destabilising political actions in cyberspace		Criminal activities in cyberspace	