



Department of Political Studies

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

Master of Arts

*Cybersecurity provision: a typology of cybersecurity
agents*

By

Kwenzokuhle Maphumulo (3619257)

Supervisor: Prof. Joellen Pretorius

November 2021

Contents

Abstract.....	5
Acknowledgements.....	6
Chapter 1: Introduction.....	10
1.1.Introduction.....	10
1.2. Background of study.....	12
1.2.Problem statement and research question.....	15
1.5. Importance of research	17
1.6. Methodology.....	19
1.7. Delimitations.....	21
1.8. Thesis structure.....	21
1.9. Conclusion	23
Chapter 2: Cyberspace and cyber insecurity.....	24
2.1. Introduction.....	24
2.2. History of cyberspace	25
2.3. Initial cyberspace adoption and use.....	28
2.3.1. Browsers	29
2.3.2. Electronic Commerce (E-commerce).....	30
2.4. Cyberspace expansion drivers	31
2.4.1 The value of internet companies.....	31
2.4.2. User growth	32
2.4.3 Mobile applications	32
2.4.4. Internet of Things (IoT)	33
2.5. Insecurity in cyberspace	33
2.5.1. Phishing	34
2.5.2. Cyber warfare	34
2. 5.3. Cyber weapons.....	35
2.6. New threats	35
2.7. Conclusion	36
Chapter 3: Cybersecurity provision: Theoretical and conceptual framework	37
3.1. Introduction.....	37
3.2. Narrow and broad conceptions of security	38
3.3. Civilising cybersecurity	40
3.3. 1. Civilising security.....	40

3.3.2. Civilising cybersecurity	42
3.4. Cybersecurity: a broad definition	44
(i) Technology and the economy	45
(ii) Politics	47
(iii) Science	47
3.4.1. Interconnectedness of spheres	48
3.6. Conclusion	52
Chapter 4: Illustration of typology of cybersecurity agents and application.....	54
4.1. Introduction.....	54
4.2. Types of cybersecurity agents	55
4.2.1. First-order political agents.....	55
A) Actor name: United States of America Department of Justice (U.S. DoJ)	55
B) Agent name: United States of America Cyber Command (USCYBERCOM).....	56
4.2.2. First-order technological and economic cybersecurity agents.....	57
4.2.2.1. Technological cybersecurity agents.....	57
A) Agent name: Microsoft.....	57
4.2.2.2. Economic cybersecurity agents	57
A)Agent name: Y Combinator.....	57
4.2.3. First-order scientific cybersecurity agents.....	58
4.2.3.1. Scientific agents.....	58
A)Agent name: National Science and Technology Council (NSTC).....	58
A) Agent name: Digital citizens alliance.....	58
4.2.5. Second-order technological and economic cybersecurity agents	59
A) Agent name: All Tech Is Human (ATIH).....	59
4.2.6. Second-order scientific agents.....	60
4.3. Threat analysis and response	62
A) Distributed Denial of Service Attack (DDoS).....	62
B) Ransomware attacks	63
C) Cybersecurity and democracy.....	64
4.4. Conclusion	67
5.1. Introduction.....	68
5.2. Summary of argument	68
5.3. Limitations	70
5.4. Areas for future research	70

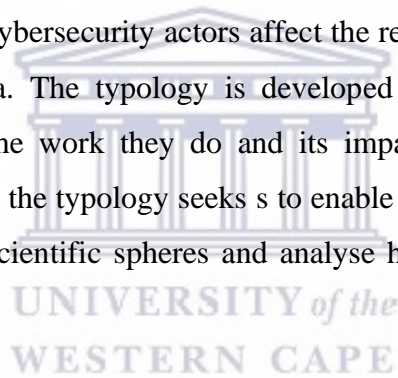
5.4.1. Domestic application	70
5.4.2. Case study application	70
5.4.3. Comparative studies.....	71
5.5. Conclusion	71
6. Reference List.....	72



Abstract

The means of communication available to humanity have evolved throughout the centuries and have become more efficient and effective. Through these changes and growing benefits, there have also been growing risks for communication and its infrastructure. With these increased risks, governments, businesses and increasingly civilians have sought to better their security in cyberspace.

Various actors are involved in the provision of cybersecurity, while other actors ensure the provision of cybersecurity itself does not negatively affect human rights and democratic norms. The thesis seeks to develop a typology of cybersecurity agents and analyse the extent to which the actions and relationships of key cybersecurity actors affect the realisation of a secure cyberspace in the United States of America. The typology is developed to enable the classification of cybersecurity agents based on the work they do and its impact on cybersecurity. Based on broadened conception of security, the typology seeks to enable easier identification of agents in the political, technological and scientific spheres and analyse how they engage with each other regarding cybersecurity.



Acknowledgements

I would like to begin by thanking the organisations that have supported me financially in my academic journey. The financial support of the Mellon Mays Undergraduate Fellowship and the University of the Western Cape Centre for Humanities Research has played a pivotal role in helping me pursue my academic ambitions. I am grateful.

To my supervisor, Professor Joelen Pretorius, I would like to thank you for making this research possible. Your assistance and guidance in helping me develop the typology, identify gaps in the field and focus my arguments is greatly appreciated. I would also like to thank you for your undying passion and perseverance throughout this research journey and the many challenges it has come with.

I would also like to extend my gratitude to all departmental staff, especially Mrs Nadia Jansen and Mr Ashley Rooks. Thank you.



To my sister, Philisiwe Maphumulo, I would like to thank you for your support and motivation throughout this journey.

To my beautiful wife, Lindelwa Maphumulo, your patience, support and understanding during this difficult period has been greatly appreciated. Your support has been paramount in making this research possible. Thank you.

To my daughter, Mbewenhle Maphumulo, and my son, Culolethu Maphumulo, thank you for adding so much colour and meaning to life. Uyanithanda uBaba.

To my good friend, Chace De Villiers, thank you for your assistance with the editing of my thesis.



Acronyms

AI-Artificial Intelligence

ARPA – Advanced Research Projects Agency

APARNET – Advanced Research Projects Agency Network

ATIH – All Tech Is Human

AUCCPDP – African Union Convention on Cybersecurity and Personal Data Protection

BBN – Bolt, Beranek and Newman

BRICS – Brazil, Russia, India, China and South Africa cooperative group

CERN – Conseil Européen pour la Recherche Nucléaire

CSIRT – Computer Security Incident Response Teams

DCCP – Digital Connectivity and Cybersecurity Partnership

DDoS – Distributed Denial of Services

DHS-Department of Homeland Security

DNS – Domain Name System

EU – European Union

EUCA – European Union Cybersecurity Act

FBI-Federal Bureau of Investigation

GDP – Gross Domestic Product

IC3 – Internet Crime Commission

ICT – Information and Communications Technology

ICCPR – International Covenant on Civil and Political Rights

IMP – Interface Message Processor



IoT – Internet of Things

ITU – International Telecommunication Union

MIT – Massachusetts Institute of Technology

MLP-Multi-Layer Protection

NATOPCD – North Atlantic Treaty Organisation Policy on Cyber Defence

NCSA – National Center for Supercomputing Applications

NYU-New York University

ONS – Office for National Statistics

PC – Personal Computer

R and D – Research and Development

RICPCRIA – Regulation of Interception of Communications and Provision of Communication-Related Information Act

SET – Science, Engineering and Technology

SSL – Secure Sockets Layer

UCLA – University of California Los Angeles

UK-United Kingdom

UN – United Nations

USDoJ – United States Department of Justice

WAN – Wide Area Network

WWW – World Wide Web



Chapter 1: Introduction

1.1. Introduction

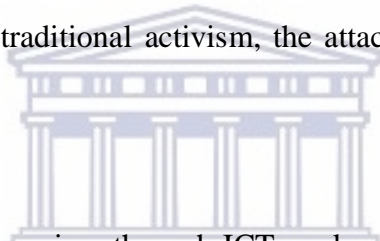
Cyberspace has become a gateway that has enabled many opportunities for humanity to be more connected and more efficient whilst enabling some industries to improve their operations. Above this, new industries have emerged and expanded exponentially with the growth of cyberspace. The growth of cyberspace has enabled a new way of living as people, businesses and governments are now able to communicate with ease without being limited by time, space and finances. As such, more organisations and people have adopted the use of software and hardware cyberspace technologies such as web services, computers, mobile phones, tablets, and a host of other devices and services currently available on the market. There are also efforts to develop new technologies that will rely on the internet such as autonomous vehicles, automated manufacturing, and software development powered by artificial intelligence among many projects currently under-way.

Improvements and increases in the availability of infrastructure and resources have allowed for increased connection at lower price points. The increase in the number of people and organisations that use cyberspace has resulted in a new category of crime known as cybercrimes or cyberattacks. Uma and Padmavathi (2013: 390) define these crimes as a “disruption of integrity or authenticity of data or information is termed as computer network attack or cyber-attack. The malicious code which alters the logic of the program and that causes errors in the output”. These crimes range from ransomware attacks to deception, commonly referred to as ‘phishing’ distributed denial of services (DDoS) attacks and a host of others. Ransomware attacks compromise a victim’s computer by encrypting the files and applications on the computer and limiting the use of the device. The attacker then requires the victim to pay a ransom to regain access to their files, applications and full use of their device (Gazet, 2010). Ransomware, DDoS and other similar attacks are mainly used to target the databases, files and applications of governments and corporations to steal data or demand ransoms.

Another type of common internet crime works by conducting what is known as online scams. These crimes mainly involve the theft of the identity of an individual or organisation. Here, victims are duped into believing they are dealing with a particular organisation or individual and are required to pay for what they believe are legitimate goods or services. In other cases, the victim is made to believe that the person they are interacting with is someone with whom they can enjoy a (financial, business, mentor, romantic, *et cetera*) relationship. Phishing described by Dhamija, Tygar and Hearst (2003: 581) as “the practice of directing users to fraudulent websites” is a cybercrime that mostly affects individuals and has been responsible for the loss of substantial losses of data and money.

The perpetrators of cybercrimes are referred to as hackers or cybercriminals. These individuals can act in groups or individually when carrying out attacks against high profile individuals, organisations and governments globally. Such individuals and organisations have successfully infiltrated and disturbed the operations of organisations and governments recently seen in the United States of America, the Republic of South Africa and Japan. The cost of cybercrime for these three nations and others, their businesses and citizens. The losses are not only financial but also include data leaks, intellectual property theft, hindrance of operations, exposure to an increased number of attacks, system vulnerabilities, viruses and other threats. Globally, the cost of cybercrimes was conservatively estimated to be USD\$375 billion in 2014 and was thought to be possibly as much as USD\$575 billion (Ganan, Ciere and Eeten, 2017: 3). It is estimated that an excess of 800 million records were lost in 2013 with costs hard to quantify due to the varying value of the records and information contained in them (Ganan, Ciere and Eeten, 2017: 3). Capturing the full scale of cybercrime on any organisation or nation is difficult as the statistics rely on the crimes being reported, which does not happen at times and the victim is unaware in some cases. Other reasons for not reporting such breaches, especially for companies, is due to the negative financial impact the company could face due to a loss of intellectual property, loss of customer records, exposure of financial records and a loss of faith by investors (Ganan, Ciere and Eeten, 2017: 1)

There is also another group of individuals and organisations who use their technical skills and knowledge as a means of protest. These groups focus infiltrating the systems of governments and other influential organisations. These activist groups target the systems of others not for ransom, data breaches or other forms of gain, but this is done as a means of protesting a particular issue or state of events. These people and groups are referred to as hacktivists. Hacktivism is a form of activism against civil, political and other injustices through hacking. Jordan and Taylor (2004: 1) describe hacktivism as “grassroots political protest with computer hacking. Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaches out of cyberspace utilising virtual powers to mould offline life”. This complex nature of attacks between private individuals and groups against states and large organisations forms part of cybersecurity and warfare architecture. Cyber warfare refers to the usage of ICT infrastructure in order to disturb political and economic stability, health and government services, and other socio-economic necessities. Like traditional activism, the attacks are carried out to persuade a change in position or action.



The disruption of these and other services through ICT are known as cyberattacks. Such attacks usually target but are not limited to “important networks affecting government, civil information, and financial markets, all institutions which underpin modern life” (Jurich, 2008: 276). These events and developments have prompted a response from multiple spheres of society which this thesis seeks to investigate. The thesis seeks to investigate how the relationships between key cybersecurity actors affects the realisation of cybersecurity in the USA by assessing the roles and responsibilities of actors.

1.2. Background of study

The current state of communication technology is the result of many years of evolution. Maryska et al. (2012: 1061) states that “ICT (Information and Communications Technology) is one of the most important factors for development and economic growth in the globalised economy”.

Communication and its related infrastructure have and continue to be of great importance for governments, businesses and civilians. The means of communication available to humanity today are more efficient and effective than what has been previously available. The production costs are significantly lower, the technology is more reliable, related services are much cheaper and the quality of the produced audio and imagery is extremely high.

“Those seeking to communicate internationally could choose the mail, or the telegraph carried over submarine cables or, after the 1900s, the radio-telegraph” (Hills, 2006: 197). From early methods such as postal services, telegraphs and printing press, the communication technology available today allows for much broader mass communication in the form of the radio and television which has been further enhanced by cyberspace and related technologies. Computer networking and the internet have significantly changed the landscape of society. An increase in the availability and capabilities of wireless communication technology, mobile networks and improvements to devices have allowed for the emergence of a new era of communication.

Writing about the risks that have come with new technological developments, Usman and Shami (2013: 192) write, “advancements in wired and wireless communication and availability of low-cost interoperable devices have resulted in development of many applications”. The developed mobile and web applications have allowed for more to be done on handheld devices such as mobile phones and tablets and portable devices such as laptops, including making purchases and processing sensitive such as identity numbers and banking details. “Trends in mobile technology that have increased access for the public include competitive data prices, lower cost Android devices, and lite app technologies that are designed to run efficiently in low-bandwidth environments” (Zamora, 2020: 53). The increased individualisation of communication technology first through personal computers and later through smartphones saw an increased number of internet users. Through these changes and growing capabilities, there have also been growing risks in the use of communication technology and its infrastructure.

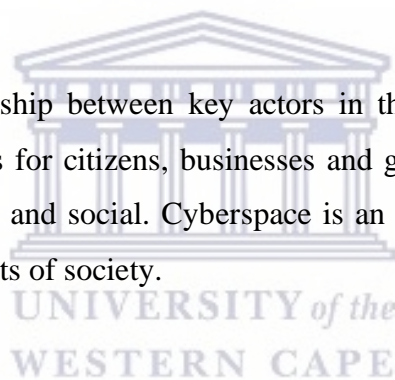
As such, this has resulted in enhanced efforts to create more effective and accepted legal standards, the improvement of the skills of the professionals to facilitate the ability to carry out offensive and defensive work in cyberspace among other efforts. These efforts have served as a catalyst for a number of global, regional, bilateral and multilateral cooperation agreements between governments, multi-governmental organisations business and civil society in varying combinations.

Attacks on a number of key socio-economic industries such as finance, oil and gas, healthcare services and more have resulted in the collaboration of all spheres of society for the development of cybersecurity legislation and coordinated response mechanisms to ensure the safety of all users and limit potential disruption. Initially, cybersecurity, responding to cyber-attacks and data breaches was seen as the duty of the government. As such, legislation and response development were taken unilaterally by governments with limited input from civil society and industry. The interconnected nature of cyberspace has seen increased cooperation between governments, businesses, civil society organisations and civilians. Different spheres of society are constantly working together in different combinations, stages and levels in trying to ensure the safety of all internet users. There have been a number of national, continental and international efforts which include but are not limited to the development of legal frameworks, setting up of response centres, research cooperation, responding to attacks and other various endeavours. As such, various actors have played different roles at different times based on their varying capabilities, knowledge and capacities. There has been an increasing number of multilateral efforts to make cyberspace and related technologies safer and more secure. These include efforts such as the African Union Convention on Cybersecurity and Personal Data Protection (AUCCPDP), European Union Cybersecurity Act (EUCA), and the North Atlantic Treaty Organisation Policy on Cyber Defence (NATOPCD).

These developments have led to a growth in research on strategies for different countries based on their unique conditions such as education levels, economic conditions, internet adoption, infrastructure and other factors.

There has been a growing body of literature regarding the roles and responsibilities of the individual users, groups and bodies involved in the creation of an international cyber response. The development of ICT has outpaced the development of legal frameworks as these are still in their developmental phase. There still remains room to contribute to the understanding of how agents in the political, technological, economic and scientific spheres engage with each other regarding cyberspace and cybersecurity as they are the key actors involved in the realisation of cybersecurity. Important to this undertaking is an analysis of how state and non-state actors provide security through policy, regulation and policing. In addition, this study also includes those actors who scrutinise cybersecurity measures and the extent to which they are democratic and respectful of human security and human rights.

The investigation of the relationship between key actors in the provision of cybersecurity is important as it bears implications for citizens, businesses and governments. These implications range from economic to political and social. Cyberspace is an important factor in the efficient operation of these three key aspects of society.



1.2. Problem statement and research question

Globally, there are increasing efforts aimed at the improvement of safety in cyberspace for a number of domestic and international reasons as it pertains to individual states. As such, multiple actors are involved in the provision of cybersecurity nationally within a state and internationally in collaboration organisations from other states. Due to the multiplicity of actors and overlapping responsibilities, there is yet to be a development of clear and concise typology that enables the analysis of all actors involved in the provision of cybersecurity within a particular region of with regards to a particular cybersecurity incident. The shared nature of cyberspace results in a shared responsibility for its safety which can “lead to ineffectiveness and replication of work” at a local and international level (Du Toit, Hadebe and Mphatheni, 2018: 120).

As such, this has resulted in an absence of clarity regarding the roles of different actors, the scope of the scope of their responsibilities, capability expectations. The absence of such a tool makes it increasingly difficult to develop national and international response mechanisms. Cavelti and Wenger (2019) provide the foundational work for the development of such a typology in their 2019 paper titled “Cybersecurity meets security politics”. This thesis seeks to build on the work of Cavelti and Wenger (2019) by assessing how the relationships between key actors in the USA affects the realisation of cybersecurity and developing a typology that can be adapted to answer questions of a similar nature in different countries and operational settings. Thus, the specific problem is in outlining who the cybersecurity agents are, their responsibilities and how their actions impact the cyber domain and civilising cybersecurity provision.

Speaking through the International Covenant on Civil and Political Rights (ICCPR), the United Nations (UN) committee highlighted its concern about the “relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act” (Sutherland, 2017: 92). The committee highlights further concerns about bringing into effect of important acts related to cybersecurity, safety and privacy. These concerns were made in response to the periodic review of South Africa by the ICCPR. Although issued in response to legislative developments in South Africa, these concerns are true for most nations, especially those that are developing and those that do not subject themselves to external audits.

The research question is therefore: How do relationships between key cybersecurity agents affect the realisation of cybersecurity in the United States of America?

Sub-questions include the following:


What is cybersecurity? and

What are the roles of key cybersecurity agents?

1.4. Research Aim

This thesis aims to analyse the extent to which relationships between key cybersecurity actors affects the realisation of cybersecurity and develop a typology of cybersecurity agents that can be deployed when trying to conduct an analysis of cybersecurity agents and the effect they have on the realisation of cybersecurity. Through its broad and internationally applicable approach, the contribution of the research will be that the developed analytical tool can be applied to any given context. This will happen by looking at the roles, responsibilities and contributions of actors in the political, technological, economic, scientific spheres. The study seeks to map which actors are securing cyberspace as a domain of human interaction through policy, regulation and policing and applying this to the case of the USA as proof of concept.

1.5. Importance of research



The international community faces several problems and hindrances in its bid to try and realise a secure cyberspace where all individuals, organisations and governments work in unison in ensuring that all are aware of their rights, responsibilities and actions they can take to ensure the security of all. These problems include but are not limited to: a lack of skills, lack of knowledge, lack of resources, low levels of collaboration between governments, national and international organisations, civil society and the general population. This has led to a legislative framework that lags behind the technology it seeks to regulate. These limitations are also noted in the South African Cybercrimes Bill of 2016. “Cooperation is impeded by difficult legal questions and “a lack of trust among community members”. CSIRTs (Computer Security Incident Response Teams) face both external and internal challenges because national laws on data localization exchange and jurisdiction may bar information sharing” (Dsouza 2017: 214).

These issues compounded by a lack of political will and other such similar problems which stifle collaboration and result in insecurity (Sutherland, 2017). It is the lack of resources, absence of

collaboration and overlapping roles of the various actors involved in cyberspace that has motivated this study. The study seeks to analyse who the agents of cybersecurity are and that for which they are responsible. Through its analysis of cybersecurity agents and their relationships, the study will be able to look at how cyberspace is being civilised as a domain of human interaction through policy, regulation and policing. The study will also analyse how some agents are civilising cyberspace by checking that cybersecurity provision is democratic, transparent, and equitable and does not violate any human rights or commonly held values. With this, the study will look at the roles and contributions of actors in the political, technological/economic and scientific spheres.

There has been a growing body of literature that is analysing cybersecurity efforts domestically and internationally. Literature has been assessed to establish where actors and nations stand in relation to cooperative efforts. Important in this literature is what nations and organisations can do to bridge the gap and increase cooperation. This study aims to contribute to this growing body of literature. As noted by Du Toit, Hadebe, Mphatheni (2018), nations take some of their policy cues from other nations such as the Brazil, Russia, India, China and South Africa cooperation agreement (BRICS), European Union (EU) and the United States Department of Justice (USDoJ). This is important to note as the internet is a shared space where events in one area can possibly affect another.

Another closely related factor and important contribution of the study is that it will allow for the systematic analysis of cybersecurity provision through a typology of cybersecurity agents. Such an analysis can help actors such as governments, civil society, academia and others to identify gaps in their provision of cybersecurity and in turn encourage better engagement between cybersecurity actors and enable the development of institutions, legislation, skills development, devolution and among other applications.

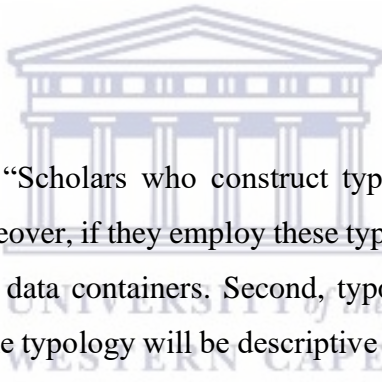
1.6. Methodology

Methodology is an important part of research as it has bearing on the reliability and validity of the study being undertaken. Important elements of the methodology include the type of research, data collection method, data analysis method and extends to other tools and materials used and the rationale that informs the deployment of these. The type of research being carried out by this study is qualitative and exploratory. The research will make use of a qualitative method as the data to be gathered and analysed will be non-numerical. The focus of the data and its analysis will be centred on the roles and responsibilities of various actors in the domestic cybersecurity landscape through identification, description and explanation.

Reiter (2013: 4-5) defines exploratory research as research which seeks to “provide new and previously overlooked explanations and it can do so by actively engaging the researcher in a process of amplifying his or her conceptual tools and allowing him or her to pose new questions and provide new explanations by looking at reality from a new angle”. Thus, this study seeks to clarify and define the nature of the problem, namely, how do the relationships between key cybersecurity actors affect the realisation of cybersecurity? The study will aim to provide a comprehensive exploration of cybersecurity incidents and develop a cybersecurity analysis typology. The study will not claim to be conclusive, rather it will be a systematic start that develops a typology and leaves room for further investigations. In line with this, the aim is to better the understanding of the issue of cybersecurity in terms of its provision and ascertain as to who the responsible parties are conceptually with an exploratory attempt to illustrate the analytical framework that the typology makes possible by using case studies. The typology will be developed through a thematic analysis which will categorise agents from cybersecurity fields in to first and second order agents. Such analysis and categorisation will be based on the work done by the various actors and their vested interests.

Collier et al. (2012: 217) define typologies “as organized systems of types—are a well-established analytic tool in the social sciences. They make crucial contributions to diverse analytic tasks: forming and refining concepts, drawing out underlying dimensions, creating categories for classification and measurement, and sorting cases”. The construction of the typology of cybersecurity agents will be in the form of a matrix which will super impose the work of Cavelti and Wenger (2019) to that of Loader and Walker (2007). The typology will marry the two works in order to create categories to classify various cybersecurity agents. The cybersecurity agents will be selected and categorised based on two criteria:

1. Their sociological location and area of operation
2. Their relationship to ‘civilising security’ by which they can either be categorise as making the domain of cyberspace safe for users or safeguarding users against security measures that may impact on their human rights.



Collier et al. (2008: 159) write, “Scholars who construct typologies necessarily are working systematically with concepts. Moreover, if they employ these typologies to classify cases, then the cells in the typology are, indeed, data containers. Second, typologies focus specifically on the relationships among concepts”. The typology will be descriptive in nature as it aims to classify the types of cybersecurity agents that exist and present the relationship that exists between the various actors involved in cyberspace. The study will make use of primary and secondary data as the study is a desktop study. Primary sources include government documents, such as legislation and policy documents, and reports. Secondary sources include books, textbooks, newspapers, academic and trade journals and websites. The use of online sources, including online library resources, is key in ensuring that the study provides the most recent and relevant information as this is a rapidly evolving area of study. The use of online sources allows the study to access vast amounts of information from various parts of the country and the world in a short space of time.

The data collected by the study will be analysed using a thematic and case study analyses that will be informed by the matrix that will be developed later in this study. Data analysis works by looking

for patterns that arise from a particular dataset and seeks to analyse the meaning of the arising pattern. The common themes that arise from the data represent an important element towards understanding the problem being researched and also play a fundamental role in helping a researcher answer their research question. Being able to identify the key themes in the literature helps in ensuring a focus on that which is most important to answer the research question. The study is further descriptive in that it will describe the themes that contribute to an understanding of the types of cybersecurity actors based on their roles and responsibilities in providing cybersecurity.

1.7. Delimitations

The study will focus on incidents of cybercrime and attacks in the USA as a means of case studies to illustrate the intertwined relationships between the various actors and how their interactions impact the realisation of cybersecurity. The study will also investigate the roles and responsibilities of actors in the political, technological, economic, scientific spheres that provide cybersecurity. In light of these delimitations that have been set, all literature and other information sources to be deployed in this study will have a clear and direct relationship to the question being asked and the topic being pursued.

1.8. Thesis structure

The thesis is structured as follows:

Chapter 1: The first chapter of this thesis has introduced the nature of the problem that is to be investigated. The chapter has also provided the research question (with sub-questions) and the research aims. The chapter has provided a background to the problem and also presented the problem statement. The first chapter has also stated the importance of the research and stated the methodology that is to be used in the carrying out of the study. The delimitations of the study have also been presented.

Chapter 2: The second chapter of the thesis will conduct a broad analysis of cyberspace. The chapter will present the background and history of the internet as we know it today. The chapter will also look at the many uses that the internet has come to encapsulate. Above this, will also be an outline of the major events that have shaped the landscape of cybersecurity.

Chapter 3: The third chapter will present the theoretical perspective that is guiding the study. The chapter will make use of the work of Cavelti and Wenger (2019) to present the first criteria of classifying cybersecurity agents, namely, the social spheres or areas of operation of the various actors that provide cybersecurity. The chapter will then move to employ the work of Loader and Walker (2007) to show how their notion of civilising security can be employed to develop the second classification criteria for cybersecurity agents, namely, civilising cyberspace by providing security in this domain or civilising the provision of cybersecurity by holding cybersecurity agents to certain human rights and principles.

Chapter 4: The fourth chapter will present the typology in the form of a matrix by superimposing the two classification criteria. It is here that greater detail will be provided regarding the roles the actors from the different spheres play in relation to the civilising of the cyber domain and the civilising of cybersecurity and examples of the different types of actors will be provided to illustrate the typology. Above this, the chapter will also provide an analysis of the impact the relationships and actions of cybersecurity actors have on the realisation of a secure cyberspace.

Chapter 5: The fifth chapter will conclude the study and summarise the findings. The chapter will also make recommendations for future research.

1.9. Conclusion

The chapter has introduced the issue of cybersecurity provision and the roles and responsibilities undertaken by various actors in ensuring cybersecurity and adherence to human rights and democratic values. The chapter has provided the background to the issue, the motivation for the study, the research question and the research aim. The chapter has also presented the methodology to be deployed in the undertaking of the study while the delimitations of the study were also outlined. The importance of the research and the structure was also presented. The research thesis will now move to present the second chapter of the thesis which will be focus on the history and use of cyberspace.



Chapter 2: Cyberspace and cyber insecurity

2.1. Introduction

The development of the internet to its current state has taken many years of research and development which has increased rapidly due to the establishment of dedicated centres and organisations. Artificial intelligence (AI) has increased the speed at which research is conducted and has allowed for further advancements in various fields from medicine to technology. “Artificial Intelligence is a branch of science and technology that creates intelligent machines and computer programs to perform various tasks which require human intelligence. It is a system that mimics various functions which a human can do” (Anjila, 1984: 65).

The internet and its related technologies have become an important feature of human existence in the 21st century. The internet and its related technologies have come to be referred to as ‘cyberspace’. Cyberspace has become a term that is prevalent in the modern era due to the importance of the technology. The term encompasses a wide range of technologies that include both software and hardware. These new technologies have affected all aspects of human life. Cyberspace is a “world of networks of computers linked via cables and routers (similar to telephone connections) which enable us to communicate, store and retrieve information. By far the largest and most well-known of these is the Internet—originally used for email, ftp (file transfer), bulletin boards and newsgroups, and telnet (remote computer access), and now even more of a household name courtesy of the World Wide Web (WWW), which allows simple stress-free navigation of the network” (Bryant, 2001: 139-140).

The expansive adoption of the internet technologies and projected growth make it important to understand the history of cyberspace technology. This chapter aims to present an in-depth timeline of the history of cyberspace in order to facilitate an enhanced understanding of what cyberspace is, its founding purpose, new threats and risks related to the increased adoption of cyberspace.

2.2. History of cyberspace

The initial computer utility was to allow users to have the ability to “gather, store, process, program, retrieve, and distribute information and to transmit text via terminals interconnected to a large central computer” (Bickerstaff, 1999: 37). The central computer was a data storage facility which handled all of the information pertinent to the users connected. There were different and separate central computers for various specialties, interests and professions. The military, universities and some professions had their centralised computers which were not connected to one another and did not allow for the cross-sharing of information (Bickerstaff, 1999). The internet, which had started through APARNET (Advanced Research Projects Agency Network), was created in response to this shortcoming in the existing system. The internet was created to help bridge the gap and allow for all users to be connected to one network and be able to cross-communicate and share information.

The internet has its foundational roots in the APARNET which was a project by the government of the USA, private corporations and institutions of higher learning that sought to research packet-switching communication between computers. The ARPANET was created in 1966 by a USA government agency named ARPA (Advanced Research Projects Agency) in a bid to create a “Wide Area Network” (WAN) linking universities and research centres. “The network consisted of individual computers or nodes on a single private line network and connected certain military personnel and defense contractors” (Bickerstaff, 1999: 39). The network began as a closed domestic project aimed at using packet switching to communicate on multiple computers at various distances. The project gradually grew with the addition of more domestic computers and the addition of computers from the United Kingdom (UK) and other European countries.

According to Leiner et al., (2009: 23), “The first recorded description of the social interactions that could be enabled through networking was a series of memos written by J.C.R. Licklider of MIT (Massachusetts Institute of Technology) in August 1962”. Licklider’s work served as a foundation

for the formation of “interconnected set[s] of computers through which everyone could quickly access data and programs from any site” (Leiner et al., 2009:23). This work allowed for growth and further research in the domain of packet switching. Increased capabilities and information on packet switching communication led to increased effort and resources being invested in advancing knowledge about the technology and further innovation. As such, a number of studies were conducted and a number of research papers written to test the feasibility of various proposed methods to establish a wider network of connected computers. One of the major debates in the early stages of trying to establish a wider network concerned establishing whether packet switching technology or circuits were best suited as the means of communication between computers (Roberts, 1978).

Multiple experiments were conducted to determine which was most efficient. It was found that “packet switching unequivocally provided efficient use of communication lines. It was clearly an economical and reliable alternate to circuit: switching, the basis for the Bell Telephone system” (Beranek, 2007: 10). Through time, more organisations became involved in the development of the ARPANET and with organisations such as Bolt, Beranek and Newman (BBN), University of California Los Angeles (UCLA), Network Analysis Corporation and others joining the initiative. The new organisations assisted in hardware development, the building of a network information centre, creating host products and others (Abbate, 2000). The first Interface Message Processor (IMP) was installed at UCLA and the first host computer was connected. More computers were connected onto the network which led to an increase in the adoption of the technology. Emails and calculations were the primary uses for computers in the early 1970s, With the technology being increasingly adopted, more capabilities were added to emails which included “selectively read, file, forward, and respond to messages” were added (Leiner et al., 2009: 24).

“The ARPANET was transferred by DARPA to the Defence Communications Agency (now the Defence Information Systems Agency) as an operational network” (Cerf and Aboba, 1993: 4). The increased traffic between devices on the APARNET and connection to satellite communication technology led to the evolution of the APARNET to become cyberspace as it is now known. As

such, cyberspace is regarded as a process of innovation. The initial stages of an open network brought about a range of communication issues between computers at great distances as some of the data packets would be lost and this would result in the network coming to a “grinding halt” (Leiner et al., 2009). The resolution of the communication issues between computers at a great distance allowed for the APARNET to expand in the USA as new nodes were introduced into the network. The network was subsequently linked to the first international nodes in England and Norway in 1972 (Abbate, 2000). The rapidly increasing number of users and international adoption, led to the assigning of domains in order to allow visitors of websites to distinguish between various websites that were becoming available. This was known as the Domain Name System (DNS) (Mockapetris and Dunlap, 1988: 124).

“Computer viruses have been around since the mid-1980s. Over 40,000 different viruses have been catalogued so far and the number of viruses is increasing dramatically” (Subramanya, 2001: 16). Towards the end of the decade spanning from 1980-to-1990, computer viruses and worms which negatively affected the functionality of computers became increasingly common and more widespread. The problem of computer viruses and worms led to the creation of software that was able to counter and block the viruses and worms. The development of the software led to creation of the of the computer security software industry.

The world's first World Wide Web (WWW) was created by Tim Berners-Lee. When developing the WWW, Berners-Lee was simultaneously working on developing ways to control computers remotely at the Conseil Européen pour la Recherche Nucléaire (CERN). “The first website at CERN – and in the world – was dedicated to the World Wide Web project itself and was hosted on Berners-Lee's NeXT computer” (Cern, 2019). Once functional, the software for the WWW was put into the public domain and was later released for free use. The free use release allowed for more people to have access to the internet and for more web applications to be developed.

The University of Illinois introduced the first web browser which was named 'Mosaic' under the National Center for Supercomputing Applications (NCSA) (Cern, 2019). The Mosaic browser was first released in 1993. The browser was initially only used in the research community due to its design and technical knowledge requirements. "Shortly afterwards the NCSA released versions also for the personal computer (PC) and Macintosh environments" (Cern, 2019). New versions of the web browser allowed for the integration of graphics and text which made the WWW more interactive and accessible.

2.3. Initial cyberspace adoption and use

Email remained one of the most used web services at the beginning of the decade 1990-to-2000. New internet services were launched at the beginning of the decade of which many became popular and widely used. A rapid increase in the number of users of the WWW enabled new opportunities which led to new areas of innovation and growth. A number of web-based services and applications were created in order to replace the physical means by which they were performed. The transition from physical to web-based made goods/services more accessible, popular and cheaper to access.

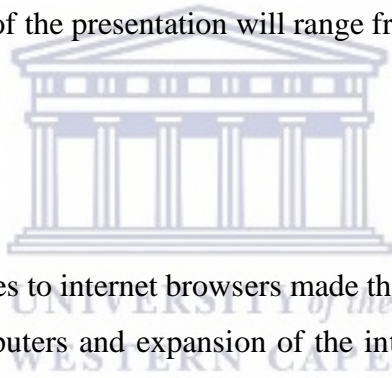


"During the dot-com bubble of the 1990s, [...] stocks were trading at record multiples of earnings. In fact, many companies with no earnings at all experienced significant increases in their stock prices during the latter half of the 1990s" (Morris and Alam, 2012: 241). Traditionally, the value at which a company's stock is traded is primarily based on its earnings and other factors too such as industry changes, and company stability, among others. Penman (2003 in (Morris and Alam, 2012: 241) described the period "of the 1990s as a pyramiding chain letter where momentum investing displaced fundamental investing". Due to the novelty of the internet and internet companies, many recently established companies within the period were perceived as being able to drastically shape the development of the industry although they would have not been able to. Due to the momentum of the time and not because of the performance of the company, large amounts of money were invested into the new internet companies; most of which failed due to a

lack of experience by the founders, competition and providing a service that was not as revolutionary as initially presumed.

The rapid growth of internet companies resulted in a five-year period from 1995 to 2000 that saw a high number of internet companies being established and soon failing after establishment. This period of rapid internet expansion and commercialisation became known as the ‘dotcom bubble’. The period of the ‘dotcom bubble’ highlighted the extent to which internet and cyberspace technology had become widely available and adopted. The following section of this thesis shall present the ways in which the technology was initially made use of. Due to the extensive scope of the deployment of internet technology, not all forms of deployment shall be presented. As previously stated, some of the innovations and inventions are still in use today and some are no longer in use. As such, the scope of the presentation will range from 1990 to 2000.

2.3.1. Browsers



The addition of graphical interfaces to internet browsers made them more accessible. An increase in the number of connected computers and expansion of the internet market led to competitive innovation of web browsers. As previously stated, the first web browser was developed at CERN, the development of the technology enabled other variants and development to browser technology. Google, owner of Google Chrome browser, and Internet Explorer from Microsoft, now Microsoft Edge, are examples of browsers that were developed during this period of early innovation and continue to exist today. After the first browser at CERN, “The Web became accessible to the general public following the 1993 release of the user-friendly graphical Mosaic browser, which led to the development of commercial applications and a user base of several million people by the next year” (Chiang, 2005: 396).

With browser technology increasingly available, a number of different browsers were created which included Line-mode in 1991, Erwise in 1992 and ViolaWWW in 1992. More web browsers

were launched in 1992 as Midas and Samba were also launched in 1992. 1993 saw the release of Mosaic, Arena, Lynx and Cello. Opera, Internet in a box, Navipress and Mozilla were all launched in 1994. In 1995, Microsoft launched the Internet Explorer browser (Hawker, 2005). This list does not capture all the browsers that were launched. The list only stated those that reached commercial success and extensive use.

2.3.2. Electronic Commerce (E-commerce)

Zwass (1996 in Molla and Licker, 2001:132) defines e-commerce as “the sharing of business information, maintaining business relationships and conducting business transactions by means of telecommunications networks”. The consumption of goods and services is an innate tenet of human existence. After research purposes, the ability to consume goods and services using the internet served as the second innovative initiative in cyberspace. The benefits to enabling shopping via the internet are many. For consumers, these include but are not limited to such as being able to view the catalogues of multiple stores at once, the ability to view and compare prices with stores in other areas/regions, being able to view and consume at one's convenience unlimited by operating hours and a range of other subsequent opportunities for business such as transportation and warehousing.

The initial cyber based services had limited adoption as the computers were not widely available due to a number of factors such as pricing, machine size, usability among other factors. The year 1994 was “a watershed year for online shopping: it's the same year Amazon launched – which, at that time, sold mostly books” (Lufkin, 2020). In 1995, eBay was launched, followed by Rakuten two years later in 1997 and China's Alibaba, in 1999 (Lufkin, 2020). The creation of the world wide web facilitated the growth of the consumption of goods and services using the internet. The integration of graphical interfaces allowed for an interactive WWW and browsers. This development allowed for the creation of e-commerce websites that were reflective and easy to use. “SSL protocol works on two layers of services where first one is SSL connection and second one is SSL session. SSL connection works at transport layer to establish links between clients and

servers. Peer to peer associations allow sessions to be built up which is ephemeral” (Satapathy 2016: 31). Secure Sockets Layer (SSL) were important in the growth of e-commerce as they enabled secure transactions, Pizza Hut was one of the first adopters of the technology as they sold “pizzas online through their early ‘PizzaNet’ portal” (Lufkin, 2020). A growth in trust and accessibility of the technology led to a growth in the number of businesses that sold goods and service “equivalent of a shopping mall in cyberspace” (Lufkin, 2020).

2.4. Cyberspace expansion drivers

Innovation has been and continues to be an important feature in the development of cyberspace technologies. The early developmental phases outlined above led to the internet becoming more widely adopted and easier to use. The innovative and inventive nature of cyberspace has continued as cyberspace has grown, these range of new inventions and innovations in web applications, advancements in mobile phone technology: software and hardware, computer technology: software and hardware, artificial intelligence and other new technologies.

2.4.1 The value of internet companies

The importance and value of the internet and internet companies to humanity are signified by the value of companies operating in this sector. The list of the most valuable companies in the world indicates which is most important to society. Of the ten most valuable companies in the world in 2020, as compiled by the American Business History Centre, the five most valuable companies in the world were technology companies. only three do not operate in the cyberspace industry (Hoover, 2020). Although not primarily technology companies, all companies on the list do make use of various technologies that are produced by the five most valuable companies and technologies produced by other lesser-known and profitable technology companies due to the ubiquitous nature of cyberspace.

2.4.2. User growth

Advances in hand-held mobile communication devices have enabled the devices to connect to the internet wireless, support browser and other mobile applications. These developments have made it possible for more people to have access to the internet. According to West (2015: 1), “over 3.1 billion people in the world have access to the Internet. This includes around 642 million Chinese, 280 million Americans, 243 million Indians, 109 million Japanese, 108 million Brazilians, and 84 million Russians”. In 2006, it was estimated that 2.5% of the African population was connected to the internet and this represented 2.2% of global internet users (Alemneh and Hastings, 2006:8). African governments and organisations with assistance of various actors are developing internet capabilities such as communication, e-commerce, software, hardware and others to help increase the number of people who have access to the internet.

2.4.3 Mobile applications

Mobile applications have enabled the accessing of cyberspace via hand-handle mobile devices. Mobile applications “consist of software/set of programs that runs on a mobile device and performs certain tasks for the user” (Islam, Islam and Mazumder, 2010: 72). The software and hardware have enabled companies to offer their services to users of smart phones. These mobile applications are commonly referred to as ‘apps’ and can be found on mobile devices, laptops and computers. As such, retailers, government departments, banks, media outlets and others have mobile applications that can be downloaded and used on-demand on mobile devices, laptops and computers. In terms of communication services, notable examples of companies making use of this technology include Facebook, Twitter, WeChat, Instagram, Snapchat among others. Concerning online consumption of goods and services, notable examples include Amazon, Alibaba, Rakuten and Jumia. A large number of banks around the world have mobile applications that allow customers to conduct banking activities on their cellphones. Mobile applications are used in many sectors for varying purposes.

2.4.4. Internet of Things (IoT)

The IoT industry is a new cyberspace innovation that allows for the control and accessing of various devices and appliances remotely. According to Woortmann and Fluchter (2015), it was estimated that the IoT industry would be worth \$7.1 trillion. Woortmann and Fluchter (2015) further argue that the IoT sector has played an important role of innovating in cyberspace. A number of the leading technology companies such as Samsung, Huawei and Google have and continue to develop IoT products. The creation of a new sector has led to the establishment of new companies such as Arm, Tive, Enovo, Samsara, Vates and others. Such companies have played a key role in the innovation of existing products and creation of the necessary software that ensures the functioning of devices with increased capabilities.

Definitions of IoT are contested. Some definitions focus on things that become connected to the internet, while others look at the “internet-related aspects of the IoT, such as Internet protocols and network technology”, and others focus on the data collection and storage definition of IoT (Atzori et al., 2010 in Woortmann and Flüchter, 2015). The International Telecommunication Union (ITU) for instance now defines the Internet of Things as “a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies” (ITU, 2012 in Woortmann and Fkucher, 2015: 223). The IoT encompasses the above approaches in those aspects of cyberspace work in tandem to enable the realisation of IoT. Hardware, software, information, network technology and other aspects are key to the functionality of the technology and future innovation. The IoT industry includes developments in the sectors of health, transportation, wearable devices, connected/smart home devices, industrial internet and oil and gas (Li, Da Xu and Zhao, 2015; Harvard Business Review, 2014).

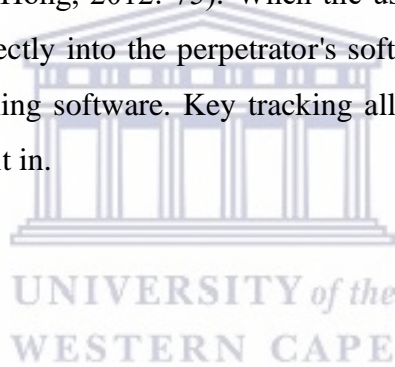
2.5. Insecurity in cyberspace

The security dilemma also extends to cyberspace with Libicki (2016: 129) demonstrating the extension in writing, “Might one country’s attempt to increase its cybersecurity come at the expense of the cybersecurity perceived by potential adversaries?”. Cyberspace has enabled a

number of possibilities and has also enabled new cyber threats. Cyber threats are complex as they allow for anonymity for the perpetrators, increased reward, lower barriers to entry, a wider pool of victims and a multiplicity of victims.

2.5.1. Phishing

According to Hong (2012: 75), phishing is the use of “social techniques rather than technical tricks to fool end-users”. Perpetrators of this crime employ social techniques such as social engineering. Social engineering attacks “aim at manipulating individuals and enterprises to divulge valuable and sensitive data in the interest of cyber criminals” (Salahdine and Kaabouch, 2019: 1). There are various methods through which the criminal act of phishing is carried out, “Another is notifying people there have been multiple failed logins for their account and they must verify their account now or risk dire consequences” (Hong, 2012: 75). When the user attempts verify their account details, they either type them directly into the perpetrator's software or the perpetrator captures their information using key tracking software. Key tracking allows the perpetrator to track the victim's information as they type it in.



2.5.2. Cyber warfare

Cyber warfare refers to the use of ICT infrastructure in order to disturb political and economic stability, health and government services, and other socio-economic necessities. The disruption of these and other services through ICT is known as cyber-attacks. Such attacks usually target but are not limited to “important networks affecting government, civil information, and financial markets, all institutions which underpin modern life” (Jurich, 2008: 276). The disturbance can be as follows:

1. A wide-scale disruption that hinders the ability of ICT to operate as per normal; and
2. The collection of data from systems with the intention to cause harm.

2.5.3. Cyber weapons

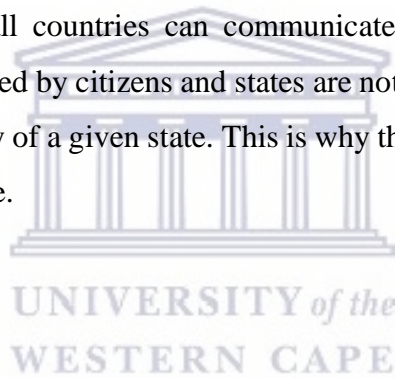
Rid and McBurney (2012: 7) define cyber weapons as “a subset of weapons more generally: as computer code that is designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings”. The definition demonstrates how computer software is used to engage in information warfare as a means of disrupting state operations or for the collection of data collection in order to cause harm against another state.

2.6. New threats

In the case of the internet, the rise of new threats on a social scale can be seen in the increased number of scams that run online that seek to dupe people out of their money and other sensitive information. These scams range from pyramid schemes that promise people wealth beyond measure, to online sales scams and also include online romance scams as well. Such internet crimes have been in existence from the time the internet became widely accessible to the general population. Writing about the nature of the issue of romance scams, Delinger (2019) writes, “According to the Federal Trade Commission, Americans lost \$143 million to romance scams in 2018, with the average victim getting scammed out of about \$2,600. The Internet Crime Commission (IC3) of the US Federal Bureau of Investigation reported to receiving more than 15,000 reports of romance scams in 2016”. The UN, 2013 (in Cross, 2015: 188) estimates that “figures are likely to undervalue the true extent of losses, given the low reporting rate of online fraud to authorities”. The victim pool for such crimes is much bigger as many do not report being scammed due to fear of being and other factors such as backlash from friends and family. The size and impact of such scams is far reaching and carries many adverse effects for the victims such financial, psychological and emotional harm. This re-configured use of the internet shows how technologies can be re-purposed when adopted by society and how this can at times lead to the rise of new threats which make the internet an unsafe space that needs to be regulated in order to ensure the protection of users and their rights. The use of the internet is at times re-configure in ways that

can be harmful and lead to loss not just for individuals, but for large organisations and nations as well.

To date, Estonia has suffered one of the greatest and most publicised cyberattacks. The attack saw the country come to a virtual standstill as many of the systems that help sustain normal day-to-day life and business grounded to a halt when the country experienced a large scale cyberattack. “The cyber-terrorist attacks occurred through the use of globally dispersed and virtually un-attributable botnets of ‘zombie’ computers. The hackers hijacked computers—including many home PCs—in places like Egypt, Russia, and the United States and used them in a ‘swarming’ DDoS strategy. Government and bank websites that normally received 1,000 visits a day crashed after receiving upwards of 2,000 hits a second” (Herzog, 2011: 52). As previously stated, the internet is a shared platform on which users from all countries can communicate and exchange ideas and other resources. As such, the threats faced by citizens and states are not only domestic, but they are also threats that lie outside the territory of a given state. This is why there is a constant need to create a coordinated international response.



2.7. Conclusion

The chapter has presented the history of the internet. The chapter has presented the various landmark moments in the development of cyberspace as it is known today. Cyberspace has grown to be an important part of humanity. The rise of the internet and related technologies has enabled new ways of living connected. The world and its information has become more accessible. And communication has become easier between people and between technology. The growth of cyberspace has enabled economic growth and the establishment of new industries. The increase in the adoption and availability of the technology has also resulted in the formation of new crimes. Cyber insecurities have and continue to negatively affect internet users. Thus, it is important to invest in cybersecurity as cyber insecurities continue to rise with the expansion of the technology.

Chapter 3: Cybersecurity provision: Theoretical and conceptual framework

3.1. Introduction

This chapter presents the theoretical and conceptual foundation that will be used to create a typology of cybersecurity agents in the USA. This typology will be used to analyse how relationships between key cybersecurity actors affects the realisation of cybersecurity. Cybersecurity can be analysed using established conceptions of Security Studies. However, the conceptualisation of security in Security Studies has been one of contention. As such, this chapter will present both the narrow and broad views of Security Studies. Such a presentation is important as the contention of this thesis is that cybersecurity is an issue that requires collaboration across both conceptions.

The chapter will begin presenting the narrow conception of Security Studies and will then move to the broader understanding of Security Studies as presented by Buzan et al. (1983). Buzan et al. (1983) presents the foundational work which moves Security Studies to issues that go beyond the security and prosperity of the state to include issues such as the environment and social stability.

Using the broad conception of Security Studies, the chapter will move to present the concept of civilising security as proposed by Loader and Walker (2007) who argue that the state has a fundamental role to play in providing security as a public good, but that the state's provision of security itself needs to be limited to ensure that it does not add to citizens' insecurity. The chapter will then move to present the different conceptual spheres in which actors can be categorised as provided by Cavely and Wenger (2019). In marrying the theoretical framework to the conceptual, the chapter will then move to present a list of the actors from different sectors of society who are involved in the provision of cybersecurity, the roles they play and how the actors link to each other.

3.2. Narrow and broad conceptions of security

The provision of security operates with two main parties in mind. The first such party is the security agent who provides security for that which or who needs to be protected. The second party is the referent object which is the party or object that requires the protection. The constantly changing definitions of who the security agent is and what/who the referent object is has seen the field of Security Studies being split into two particular camps. The first focused on the protection of the state (referent object) and saw the state as the main security agent, a traditional understanding. The second saw a shift in how security is thought about and this shift was marked by the work of Buzan et al (1983), namely, the referent object being the individual, the citizen and more recently, the preservation of the planet (Williams,2021: 3), The shift in the field of Security Studies saw the coming into existence of two perspectives in the field, a broad and narrow perspective.

The narrow perspective of Security Studies was mostly concerned “with the four S’s of states, strategy, science and the status quo. It was focused on states inasmuch as they were considered (somewhat tautologically) to be both the most important agents and referents of security in international politics” (Williams, 2012: 3). The focus on the function of the state and its protection is directly linked to the fact that the field of study came to prominence post-World War II. At its birth, the field was born into a mercantilist world marred by nationalism and the prioritizing of the state. Vasquez (1998: 37 in Guzzini, 2004: 536) “defined the realist paradigm through three tenets, namely, the assumptions of anarchy, of statism, and of politics as the struggle for power and peace”.

The realist perspective was the main informing theoretical framework for most nations after World War II as a number of nations tried to secure themselves and be prepared as best as possible for any unforeseen future conflicts. As such, there were many instances of the security dilemma taking place. The security dilemma is a situation in which a state decreases the security of another by trying to improve its own. As such, the state with decreased security tries to improve their own security which makes the initial state feel insecure. This then creates a perpetual cycle of improving

offensive and defensive capabilities (Glaser, 1997). For Leiter (2001: 245), “Classical Realism denotes a certain hard-headed, unromantic, uncompromising attitude towards the world, which manifests itself in a brutal honesty in the assessment of human motives and the portrayal of human affairs”. Realism is a theory that mainly focuses on the functions of the state such as the military protection and advocates for states to pursue their own goals as the world in which states exist is anarchical with no world government to ensure the safety and security of all states. As such, there is no possibility for mutual gain and mutually assured security. It is rather about competition and gaining more at the expense of another state. It was in the context of the realist perspective which is heavily concerned with the survival, competition and unilateral prosperity of the state that the narrow debate on Security Studies was born.

Realising the shortcomings of such a narrow perspective that disregarded the other elements of human life, efforts were made to broaden the field so that it could be more inclusive and cognisant of other security issues that go beyond the survival and prosperity of the state. Buzan et al. (1983) argued for the expansion of the field of Security Studies not in a bid to nullify the importance of the aforementioned complex, but in order to highlight other issues that are also of concern with regards to general human security and state survival. The issues as highlighted by Buzan et al. (1983) are security issues relating not only to the military but also to the environment, economic security, political stability and social stability. The argument made was that military issues and those concerned with nuclear weapons and superpowers should be moved to the field of strategic studies in order to allow the field of Security Studies to expand while enabling this important sub-field to survive.

In the expanded definition of Security Studies, Buzan et al (1983: vii) saw the field of Security Studies as being able to be expanded and further cover issues that lay under the realms of the military, politics, economic, environmental and societal issues. Such an expansion from strictly military issue to include other socio-economic issues would prove important as the Cold War drew to an end and the world in which states were existing was beginning to change rapidly. There was a growing need to address issues that lay beyond the survival of the state and the military. The call

to change focus was due to the rise of the liberal institutionalist order which saw the nations of the world move away from the pursuit of power through the primitive means of violence and competition. Nations moved towards rather seeking mutual cooperation and for shared responsibilities. The liberal institutionalist order led to shared growth, prosperity, decreased violence and greater peace. This move saw other issues come to the fore such as migration, poverty, climate change, housing, economics and a host of other issues that had been starved of attention owing to the fact that all focus had initially been placed on military capabilities and the pursuit of global dominance.

The shift from the state being the referent object to other issues, broadened the field of Security Studies. This change saw the field of Security Studies focus on issues beyond state security. Widening the scope allowed for attention to be paid to issues that were previously not seen as being security issues and the notion of human security developed. “Human security is not a concern with weapons. It is a concern with human dignity. In the last analysis, it is a child who did not die, a disease that did not spread, an ethnic tension that did not explode, a dissident who was not silenced, a human spirit that was not crushed” (Haq 1995: 116 in Williams, 2012: 7). This thesis draws on the broad conception of Security Studies in that it focuses not only on the state as a security agent and referent object of cybersecurity, but considers all actors that are involved in the provision of cybersecurity and use of cyberspace. Thus, the thesis also looks at the role of other non-state actors such as civil society, corporate and academia. This role is elaborated by drawing on the notion of civilising security.

3.3. Civilising cybersecurity

The study draws on the idea of civilising security to develop the framework of analysis for mapping cybersecurity agents.

3.3. 1. Civilising security

“Security [...] is an unqualified human good. The protection of its people from internal and external threats stands consequently as the first and defining priority of government” (Loader and Walker,

2007: 10). The protection of a country's population from harm is a key function of the state. It is important that a state is able to carry out this function along with the protection of its sovereignty. Failure to perform these two primary tasks adequately leads to instability. The state has to balance the carrying out of these functions with the human rights of the population. As such, the manner in which these duties of protecting citizens are carried out by the state is kept in check by state institutions, civil society groups and private citizens.

Security “is in a sociological sense a 'thick' public good, one whose production has irreducibly social dimensions, a good that helps to constitute the very idea of 'publicness'. Security [...] is simultaneously the producer and the product of forms of trust and abstract solidarity between intimates and strangers that are prerequisite to democratic political communities” (Loader and Walker, 2007: 8). Security is an important dimension of modern society as it civilises human existence and allows for living beyond survival. The power of security is yielded in two ways; the first is that it is the state that has the monopoly on the use of force and the second is that through the social contract of democracy and other forms of government, security is provided for all citizens which allows for a 'civilised' society.

Checks and balances in any society ensure that one group does not forcefully impose its will on the rest of society; this is true for both state and non-state actors. “States—even those that claim with some justification to be 'liberal' or 'democratic' have the capacity when self-consciously pursuing a condition called 'security' to act in a fashion injurious to it. So too do non-state 'security' actors [...] they proceed in ways that trample over the basic liberties of citizens; that forge security for some groups while imposing illegitimate burdens of insecurity upon others” (Loader and Walker, 2007: 7). At times, due to various factors, states can find themselves acting in ways that might harm one group of society while trying to ensure security. As such, it is important to have checks and balances in order to ensure equal security for all citizens.

“As modern states sought to nurture or foster national identities, police forces became deeply implicated in the wider cultural project of nation formation” (Loader and Walker, 2007: 27). The

provision of security is, as previously stated one of the main and primary duties of any state towards its citizens. Ensuring security internally and by securing the borders of a particular country is one of the most important characteristics of a state. States provision of security using means such as the police services among others civilises human interaction within their territory and contributes to the creation of national identities.

The use of a police force in order to civilise human interaction within a particular territory is the means by which the state tries to fulfil its duties towards its citizens of ensuring protection from internal threats. The military plays a role in ensuring protection from external threats through protecting borders and also through deployment in other countries to help bring about stability and avoid humanitarian and other crises. In trying to create security for its population, the state can create insecurity for certain parts of the population which is why it is important to have civil society groups and sectors of society that analyse the means through which this public good is provided in order to ensure that it does not create an unnecessary burden of insecurity for certain portions of the population. Security that fails to secure all equally is what Loader and Walker (2007) label as ‘uncivil security’. By contrasting Loader and Walker’s (2007) definition of uncivil security, the ‘civilising’ of security can be defined as security that proceeds in ways that do not trample on the basic liberties of citizens; security that does not forge security for some groups while imposing illegitimate burdens of security upon others, or extends the coercive reach of the state-and security discourse-over social and political life.

3.3.2. Civilising cybersecurity

The field of cybersecurity is a relatively new area of human life that requires security in order to protect individuals and organisations from various threats that lie in cyberspace. In cyberspace as is with the broad the definition of security, the government has a priority to protect its subjects from internal and external threats. It is important that states and their partners are able to carry out this function as the threats of cyberspace are diverse with greater population reach and harm. Failure to carry out the function of securing cyberspace can lead to a number of domestic problems

for the population, organisations and state as illustrated in chapter 2. Being able to perform this function in a transparent and reliable manner ensures the protection of human rights from external threats and internal overreach.

More particularly in the case of cybersecurity provision, the relationship between the parties involved in the security formula is different from traditional debates in which the state is the security provider for its citizens or in which the state needs to be secured from an external threat. In the case of cybersecurity, the security relationship is a symbiotic relationship in which security provision is the duty of all members of society as the actions of one can easily harm the other. As such, all actors such as the state, regional organisations, civil society organisations and others exist in a reality of constant vulnerability as the threat faced is not clear in the form one particular state or adversary, but it is a range of threats that include states, terrorists organisations, private individuals and groups who might seek to cause harm to a particular government, its people, organisations, businesses, healthcare system, etcetera.

The state has a responsibility to provide cybersecurity as a public good in cyberspace, i.e. security provision in cyberspace in the first instance attempts to make human interaction in cyberspace safe. Addressing threats such as cybercrime and cyberattacks are the first and foremost the role of the state which it does through cybersecurity law, cybersecurity policing measures and international cooperation. However, just as generally conceptualise above, this provision can impede on human rights. Such impediments are highlighted when governments limit access to certain parts of the internet as seen in China and Uganda. Other countries that limit internet access and censor the internet include Ethiopia, Cuba, North Korea, Iran and Saudi Arabia. These limitations impede on rights such as freedom of association and freedom of speech which negatively affects human security.

By extrapolating Loader and Walker's (2007) definition of uncivil security, the 'civilising' of cybersecurity can be defined as security that proceeds in ways that do not trample on the basic

liberties of citizens; security that does not forge security for some groups while imposing illegitimate burdens of security upon others, or extends the coercive reach of the state-and security discourse over social and political life. Cybersecurity is therefore, also about civilising the provision of security in cyberspace in a manner that guarantees equal security for all. Although the relationship is symbiotic, the government is still charged with playing the leading role in the creation of legislation and institutions that will provide overarching cybersecurity policies, regulations and infrastructure. Such an engagement between the state, civil society groups and other stakeholder means that cyberspace remains secure through policing and regulation while the transparency and respect for human rights by security agents is monitored by civil society groups and individuals.

3.4. Cybersecurity: a broad definition

There are multiple definitions for cybersecurity. The definitions vary across sectors and interests. Drawing from the ITU, Cybersecurity can be defined as a “collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets” (ITU, 2008 in von Solms and van Niekerk, 2013: 2-3). The referent objects of cyberspace that require protection “include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment” (ITU, 2008 in von Solms and van Niekerk, 2013: 2-3). Cybersecurity seeks to guarantee and maintain security against threats by ensuring availability, preventing replication and achieving confidentiality (ITU, 2008 in von Solms and van Niekerk, 2013: 2-3). Von Solms and van Niekerk (2013) argue that cybersecurity goes beyond the limits of information security as cybersecurity involves humans. Humans can be victims of cybercrimes or participate in the perpetration of cybercrimes with or without their knowledge. It is this involvement of humans that adds complexity to the nature of cyberspace and requires such analysis as that which is being carried out by this thesis.

This distinction in definition is important as it helps to highlight what could be labelled as the ‘broad’ and ‘narrow’ debates of cybersecurity. As in the case of human and state security, information security would be seen as the narrow perspective as it is primarily concerned with the protection of information and related infrastructure whilst disregarding the far reaches of cyberspace and its impact on society. The concept of cybersecurity contrast also factors in the many resulting effects such as social, political, environmental, economic among others. In light of this, cybersecurity cannot be analysed from a singular perspective as it has far reaching effects. Thus, to fully map out the agents of cybersecurity, this chapter will draw on the schema of Cavelti and Wenger (2019: 9), who trace the intellectual history of cybersecurity by analysing the drivers of cyberspace from three spheres of society; namely technology (development, use and key events), politics (international and domestic politics) and science (academic debates, research and development. The technological sephere has been expanded below to include the economy.

(i) Technology and the economy

Technology as a sphere of society is related to cybersecurity in two ways. The first is that the technological advancements that are made address particular needs and problems within a given society; this could be addressing a particular threat or addressing a particular problem to allow for greater efficiency. The second relation is an indirect one in which when the technology is used, it can take on other uses beyond those that the technology was initially designed for which could lead to the rise of new threats. It is this unpredictable nature of the number of uses that a technology can take which makes it a political matter as much as it is a technological (Cavelti and Wenger, 2019: 10-11).

Economic stability and prosperity are important to all and this is no different when it comes to cyber and related industries. In the same manner that strong economic positions (among other reasons) were able to enable conquest, war and industrialisation; strong economic positions are here too important to the development and innovation that happens in cyber and related industries.

Although creating and improving technology on a small scale may be possible, it is financial support that enables further research and mass adoption. The role of financial support for small and large companies is important as it allows entry into new markets, the hiring of more staff, acquiring more conducive space and a host of other related activities.

As such, this is why it is important to include the economic sector with the technological as the two are closely linked to each other. The relationship between economics and technological development is shown in section 2.3. of chapter 2 that looks at Early internet adoption and use. The relationship between economics and technology continues to prevail in the 21st century with the success of many of the new technology companies being heavily reliant on a range of economic factors beyond financial support. Governments have also come to realise the importance of technology and are investing heavily in technological research and the acquisition of the latest technology. For instance, the United Kingdom Office for National Statistics reports that the “government’s expenditure on science, engineering and technology (SET) relating to research and development grew by £0.7 billion to £12.2 billion in 2017, an increase of 6.4%” (ONS, 2017). And “China’s spending on research and development (R&D) climbed 10.3% to 2.44 trillion Chinese yuan (\$378 billion) and accounted for 2.4% of gross domestic product (GDP) in 2020, according to official statistics” (Kharpal, 2021). The spending of these two economically well-placed nations highlights government spending has changed.

Other forms of financial support for small companies have also come into being through what is known as 'crowd-funding'. Crowd-funding works through “the provision of funds through small donations or sponsoring by individuals from various Internet communities or from organisations which identify themselves with the specific project seeking funding” (Hemmer, 2011: 2). These alternatives have allowed for companies to access capital outside of established sources such as investment firms, venture capital, angel investors and others.

Thus, this is why the economic sector was added to the technological sphere as the two share close ties and are interdependent as a range of technological innovations has economic implications in various ways.

(ii) Politics

Cybersecurity initiatives require domestic cooperation between civil society, businesses and government across a wide scale. Above this, international cooperation between governments of the world and businesses is required as cyberspace is highly interconnected and negative events in one country or region can have a negative impact on another. It is with this that the creation of international legislation and institutions is important in order to ensure a well-coordinated response if and should the need arise. Moreover, most states are not in full control of important infrastructure due to free market capitalism which has allowed private corporations to thrive and has also allowed foreign companies to be suppliers of this infrastructure. The current security reality leaves states in what could potentially be a vulnerable state (Cavelty and Wenger, 2019: 12-13).

(iii) Science

The role of academia in the development of both cyber technology and cyber policy debate is paramount. The difference in approaches and opinions in the field of cybersecurity allows for an expanded understanding of the field, what needs to be done and how it should be done. The variations allow for the evaluation of different perspectives with regards to what lies beyond the immediate. Academic debate is also important to politics and technology as what arises from the debates can shape policy and legislation and can also make its way into general society which in turn will have an effect on the development and production of technology and the meanings it takes on as adoption increases (Cavelty and Wenger, 2019: 13-14). The influence of academia on society is not unidirectional, but is rather an exchange of influence as society also has an influence on what takes centre stage as research interests.

The importance of funding in academia cannot be overstated as funding plays a crucial role in giving or denying attention to particular research interests. With there being an extensive range of implications and consequences in cyberspace, room has been created in order to allow the field to grow and lead the creation of knowledge that will result in more security and innovation. There has been growing prominence given to cybersecurity initiatives. These initiatives span from small-scale community awareness projects to projects on a much larger scale driven by academics to think-tanks that seek to assist in the creation of legislation and institutions that will ensure cybersecurity. Examples in the USA of this include work being done by the Federal Bureau of Investigation (FBI), United States Department of Justice, FBI Cyber Division and other agencies.

An analysis of the agents of cybersecurity through Ian Loader and Neil Walker married with the framework of Cavelti in Wenger allows for inspection of the interconnectedness of the spheres of society and how that in turn shapes technological development and government legislation and regulation. Such an analysis will help to better understand how cyberspace is being civilized through providing security and to better know what measures are being taken to ensure the protection of human rights and freedoms.

3.4.1. Interconnectedness of spheres

The combination of these two works will allow for the creation of a typology based on two criteria, namely, firstly, the contribution being made by player in the political, technological and scientific spheres, and secondly how these contributions are enabling the civilisation of the cyber domain and the civilisation of cyber security provision. The thesis will categorise first order agents as actors that direct their energy to civilise the cyber domain while actors that civilise cybersecurity provision will be categorised as second order agents. The categorisation is not made in order of importance, but rather made in order of action. First order agents act first, mostly through legislation, policing and cyberspace development and innovation while second order agents act in response to how the first order agents seek to change the landscape of cyberspace. Second order agents respond through lobbying policy-makers, protests or creating awareness of adverse impacts

that cybersecurity provision may have on human rights and other democratic values. This will be presented in greater detail later on in the chapter.

The three spheres shape cyberspace interactions between members of society and they also shape the manner in which society chooses to respond to perceived cybersecurity threats. The broad relationship between these spheres as taken from Cavelti and Wenger (2019: 9) is as follows: Technological dynamics interact with social and political dynamics. Technological possibilities and constraints influence socio-economic processes. In turn, political preferences and contexts shape the evolution of digital technologies. This also applies fundamentally to the actors developing these technologies and to the dynamic interplay of cybersecurity markets and cybersecurity politics.

Technology as a driver in the study of security politics is related because technology develops within certain contexts in order to help address a particular problem that society is facing or to help guard against a particular threat that might be on the horizon. Technology is designed with a particular aim and focus. “In modern society, technology resents itself to society primarily through its function. All other qualities (e.g., aesthetics, spirituality, ethics) are secondary. Unlike with natural objects, this immediate perception of technology as differentiated into primary functional qualities and secondary social qualities rips technology from its social context” (Pretorius, 2008: 303). For the designer, manufacturer and technological determinist commentators the understanding held is that technology will serve its intended purpose and serve the presumed change in society. Such a view of the role of technology in society is known as technological determinism which Chandler (1995:2) defined as follows: “Technological determinism seeks to explain social and historical phenomena in terms of one principal or determining factor (technology)”. Such determinism sees technology as existing outside of society and only exerting its influence upon society and the technology itself not being influenced or shaped by the society in which it is existing.

Although designed to achieve a specific end or achieve a particular goal, technology is used in social settings in which it can come to adopt new meanings and uses as the adoption rates grow steadily as opposed to the view that technology will exist without being shaped and have re-configured use in the society in which it exists. When technology is used, not only can it take up new meanings and purposes in society in order to improve the living conditions of a society or allow for greater efficiency, but the changes in purpose and meaning can have other effects as well. When the technology takes on other uses beyond those that it was initially designed for, it can lead to a rise of new threats. It is this unpredictable nature of the number of uses that technology can take which makes it a political matter as much as it is a technological matter (Cavelty and Wenger, 2019: 10-11).

3.5. Conceptual matrix of cybersecurity provisions

Based on the frameworks of Cavelty and Wenger and Loader and Walker, a matrix to categorise cybersecurity agents can now be constructed as shown in Figure 1. The vertical axis consists of the criteria concerned with the civilising of cybersecurity and classifies cybersecurity provision in terms of civilising the cyber domain through regulating and policing activities by first order agents and civilising the provision of security itself by second order agents. The first order agents ensure security provision in cyberspace and the second order agents ensure that the provided security does not go against human rights and other democratic norms. The horizontal axis consists of the different sectors of society where cybersecurity provision operates from and in.

Figure 1: Conceptual matrix of cybersecurity provision

	Political Sphere	Technological/ Economic Sphere	Scientific Sphere
First-order agents: civilising cyberspace			
Second-order agents: civilising cybersecurity provision			

According to Calderaro and Craig (2020: 4), “The implementation of cyber capacity building strategies should also support countries in the Global South to increase their potential as active players in the transnational governance approach to cybersecurity, by developing the diplomatic capacity to negotiate norms and transnational agreements in international fora”. Actors, both domestic and international set the rules that govern internet use. These agents who act first by setting the rules, developing technology or enabling finance, are categorised as ‘first order-agents. These actors are responsible for the creation of cyberspace legislation and technology while also ensuring the creation of an internet environment in which there can be peace and safety for all users of the internet.

There are also other actors that assist the state in the creation and enforcement of laws. This ensures the meeting of internationally accepted standards. As previously mentioned, the cybersecurity agents will be selected and categorised based on two criteria:

1. Their sociological location and area of operation
2. Their relationship to ‘civilising security’ by which they can either be categorised as making the domain of cyberspace safe for users or safeguarding users against security measures that may impact on their human rights.

An international application of the typology would include actors such as the International Telecommunications Union (ITU), United Nations (UN), United States of America Department of Justice (US DOJ), European Union (EU), Brazil, Russia, India, China South Africa cooperation agreement (BRICS), North Atlantic Treaty Organisation (NATO) and other international, multilateral and regional actors. These actors are classified as first order agents as they too have responsibilities towards society. These are first order agents in the political sphere. The actors in the political sphere are responsible for enabling transnational cooperation between businesses, civil society and state organs.

There are also first order agents in the technological and economic sphere and also in the scientific sphere. Those in the technological and economic sphere are those responsible for the raising of capital to help fund innovation and invention of security mechanisms. Closely linked to these actors are those in the scientific sphere. The actors in the scientific sphere interacts with both aforementioned actors as they play a key role in legislation, research and the setting of norms. “Law enforcement agencies such as the USDoJu and the (ITU) have, therefore, initiated programmes that assist developing countries in the African, Caribbean and Pacific Group of States to draft laws and other appropriate prosecution instruments to successfully indict cybercrime offenders” (BRICS, 2017 in Du Toit, Hadebe, Mphatheni, 2018: 119).

Actors who respond to proposed/adopted laws, research in progress, developed technologies and other related matters are those the thesis categorises as ‘Second order agents’. These actors are second to act in the pursuit of secure and prosperous cyberspace. Second order agents are mainly concerned with ensuring that the first order agents act in ways that are respectful of human rights, democratic and in line with established norms. These actors too can be categorised into political, technological/economic and scientific/academic spheres. Like the first order agents, these actors range from domestic, regional to international.

3.6. Conclusion

The chapter here concluded has presented the theoretical and conceptual framework that grounds the investigation of the provision of cybersecurity and the typology to analyse cybersecurity agents in different contexts as well. The chapter began by presenting a brief evolution of the field of Security Studies. The changes in the field over time now link to cybersecurity and the provision of cybersecurity thereof to the field of Security Studies to allow for broad conception of cybersecurity. The theoretical and conceptual framework combined the work of Loader and Walker (2007) on civilising security with that of Cavelti and Wenger (2019) on the different spheres that actors who are involved in the provision of cybersecurity operate in and the roles that these actors play. In doing so, the conceptual matrix was constructed that will be used to inform the typology of cybersecurity agents in the next chapter.



UNIVERSITY *of the*
WESTERN CAPE

Chapter 4: Illustration of typology of cybersecurity agents and application

4.1. Introduction

The nature of cyberspace is one which involves and affects most spheres of society as demonstrated in chapters 2 and 3. The two chapters provided the contextual, conceptual and theoretical backgrounds for the study. Chapter 2 looked at the history of the internet and cyberspace, the current state of the technology and other developments and innovations that have arisen because of the internet. Chapter 3 presented the theoretical, conceptual and analytical framework. The framework was developed using the work of Loader and Walker (2007) on Civilising Security. The work of Loader and Walker (2007) was married to the work of Cavelti and Wenger (2019) which provides a framework that outlines the main actors that are involved in the provision and realisation of cybersecurity at a national level.

This chapter will provide a populated illustration of the typology of cybersecurity agents based on actors from the chosen geography, the USA. The chapter will present the prominent actors that are involved in the pursuit of a secure cyberspace. The chapter will then move to provide cases of cybersecurity incidents and show how the typology can be applied in order to determine how relationships between key cybersecurity agents affect the realisation of cybersecurity in the USA. There are six categories under which the cybersecurity agents can be classified. An outline of each category has been provided in chapter 3. This chapter will provide examples of agents based on the outlines provided. An analysis of the actors work and its scope will allow for the assigning of the agents to their respective categories. An argument will be provided to explain why each agent is being placed in a particular category. The chosen actors have been identified based on the work they do in the field of cybersecurity and cyberspace. The work done by these actors contributes to the realisation of a more secure cyberspace through the development of legislation, international cooperation, financial investment, development of software and hardware, advancing research and ensuring that these are done in a manner that is in line with established human rights and values.

4.2. Types of cybersecurity agents

A populated typology of cybersecurity agents is provided below to illustrate the application of the matrix to cybersecurity analysis (see figure 2). The list is not exhaustive, but will rather show how the schema is to be populated when analysing agents in the cyber domain and their effects on the realisation of cybersecurity.

Figure 2: Populated cybersecurity matrix

	Political Sphere	Technological/ Economic Sphere	Scientific Sphere
First-order agents: civilising cyberspace	U.S. DoJ USCYBERCOM	Sequoia Capital Microsoft	NSTC
Second-order agents: civilising cybersecurity provision	Digital Citizens Alliance	All Tech Is Human	Cybersecurity for Democracy

UNIVERSITY of the
WESTERN CAPE

4.2.1. First-order political agents

A) Actor name: United States of America Department of Justice (U.S. DoJ)
Established:1870

Nature of work: The US DoJ was created by Congress as “an executive department of the government of the United States”. The department was charged with handling “all criminal prosecutions and civil suits in which the United States had an interest” (Justice, 2018).

The agency has been involved in various initiatives around the world as far as justice and the development of legislation are concerned. Regarding cybersecurity law, the agency has a programme named ‘The Digital Connectivity and Cybersecurity Partnership (‘Digital Partnership’

or DCCP)’. The programme seeks to increase the number of people who have access to the internet in emerging markets, whilst ensuring that the internet is safe and secure. As such, the programme seeks to “Work with partner countries to adopt policies and regulatory positions that foster and encourage open, interoperable, reliable and secure Internet” (United States Department of State, n.d.). The approach of the agency is two-pronged, it focuses on legislation and capabilities. This is an important consideration to the approach as an absence of the necessary skills and resources can lead to a failure in the implementation of legislation and best practice. With a lead and set approach, the agency is operating as a first-order political agent through the involvement of the state machinery and interstate engagement through diplomacy and other multilateral approaches. The work of the U.S. DoJ ensures protection from external threats and allows for cooperation which is an important activity as per the broad definition of cybersecurity.

B) Agent name: United States of America Cyber Command (USCYBERCOM)
Established: 2010

Nature of work: The U.S. Cyber command was established by the department of defence (DoD) with the aim of protecting the DoD's information networks, to improve and support the cyber capabilities of the department of defence and to serve as a national cyber security incident response team by adding skills and expertise to help the United States “withstand and respond to cyber-attack(s)” (Cybercom, 2017). The command also works with allies in the carrying out of missions and other activities related to the scope of the centre. The Cyber Command also seeks to help the nation remain strategically competitive in cyberspace, defend civilian assets, compete and deter in cyberspace, cultivate talent and a range of other activities for which the command is responsible (DoD, 2018).

The U.S. Cyber Command is a first order political organisation as the organisation provides tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be use to protect the cyber environment and organisation and user assets.

4.2.2. First-order technological and economic cybersecurity agents

4.2.2.1. Technological cybersecurity agents

There is a large number of technological actors involved in the cyber domain due to the various sub-fields and expansive reach of the technology. The involved actors produce and maintain various forms of hardware and software. Due to the limits of this thesis, one prevalent technological actor from the chosen geography will be presented.

A) Agent name: Microsoft
Established: 1975

Nature of work: Microsoft is a cyberspace software and hardware development company. The company operates and offers a number of cyberspace technologies that include productivity and business processes; intelligent cloud; and "More Personal Computing" (Microsoft, n.d.). The various segments in which the company operates comprise multiple devices and services related to cyberspace. Some of these products and services are for personal use and some are for commercial use. A number of the products and services offered are for both personal and commercial use. Microsoft is one of the most important actors for computer technology as the company made it possible for more people to have access to computers. The company has been at the forefront of software and hardware development.

4.2.2.2. Economic cybersecurity agents

A) Agent name: Y Combinator
Established: 2005

Nature of work: Y Combinator is a start-up company accelerator that helps newly formed and conceptual companies receive mentorship, business education and further work on the products or services they are developing to potentially secure their company's first investor funding known as

'seed funding' (Y Combiator, n.d.). Through Y Combinator, companies receive support that allows them to become financially viable and break even. This support is important in helping companies survive and have access to more funding from more investors. The financial support provided can be up to \$500, 000 which the company can use to further research and development and to grow their user base (Y Combiator, n.d.). Y Combinator also provides other important tools and skills to newly formed companies such as office space to work in for three months, networking, access to established business people through motivational talks and interactions, first customers and more. Y Combinator has played an important role in the establishment and success of many technology companies that have become important globally such as Airbnb, DoorDash, Dropbox, Instacart and many other companies.

4.2.3. First-order scientific cybersecurity agents

4.2.3.1. Scientific agents

A) Agent name: National Science and Technology Council (NSTC)
Established: 1993



Nature of work: The National Science and Technology Council was established in 1993 to advise the president of the USA on matters relating to science and technology to help achieve the nation's goals. The council is responsible for the coordination of science and technology policies that are in line with the president's aims. The council also ensures that all agendas are integrated into all levels of government while also ensuring international cooperation on science and technology research and development (National Science and Technology Council, 2022) . The council works closely with other government agencies dedicated to cybersecurity such as the Cybersecurity and Infrastructure Security Agency, United States Department of Homeland Security, United States Computer Emergency Readiness Team, United States Department of State and many others.

4.2.4. Second-order political cybersecurity agents

A) Agent name: Digital citizens alliance
Established: 2016

Nature of work: “Digital Citizens is a consumer-focused group whose mission is to raise awareness among the public and policy-makers about how to make the Internet safer” (Digitalcitizensalliance, n.d.). It is through responsive and secondary work to give political and legal assistance that the organisation becomes a second-order political agent. The organisation “engages with key Internet stakeholders, individuals, Internet companies, and civic leaders to search for solutions to Internet safety issues” (Digitalcitizensalliance, n.d.). This sees the organisation not being able to lead the political charge, but rather assist in its establishment and revision of proposed or adopted legislation and norms. The organisation has been involved in multiple efforts aimed at raising awareness, investigations, legislators and a range of other initiatives.

There are many such other political organisations and initiatives focused on ensuring public safety, respect for human rights, adherence to democratic values, transparency. Such organisations that have an interest in ensuring that all first-order cybersecurity agents are doing what is expected of them are to be categorised as second-order political agents.

4.2.5. Second-order technological and economic cybersecurity agents

A) Agent name: All Tech Is Human (ATIH)

Established: 2018

Nature of work: ATIH is an organisation with intentions to “to grow the Responsible Technology field by promoting knowledge-sharing and collaboration among multiple stakeholders in order to co-create a better tech future” (ATIH, n.d.). The area of responsible technology is one that is relatively new with regards to ethics and standards for cyberspace. The area is the cyberspace equivalent of fair trade and conflict free products and services (Miller, 2017).

As such, the area seeks to ensure that there are established ethical guidelines and standards for technology companies that can allow users to know that the technology they consume is ethical and in line with particular standards. Examples provided by Miller (2017) of these ethics and standards include but are not limited to knowing what happens to user data gathered by mobile

applications, ensuring that advertising revenue does not fund extremism, guaranteeing originality of content, ensuring the ‘gig-economy’ pays a living wage, making terms and conditions comprehensible and a list of other various elements to be considered. The field of responsible technology is important in helping start-up companies develop their products and services in a way that is mindful of human rights and other democratic norms.

The field also allows for established companies to re-think and re-configure their products and services in a way that is mindful of human rights and democratic norms. ATIH serves as a primary example of a second order technological and economic cybersecurity actor by ensuring that cybersecurity and its related technologies do not trample on human rights or forge security for one group while creating a burden of insecurity for another group. The field also allows for the limiting of state overreach.

There are many similar organisations regarded as second-order technological and economic agents. These are organisations that focus on ensuring that the technology developed by the various first-order agents does not have detrimental effects on society, the planet, infrastructure, international relations and other important elements of modern life. Organisations with a concern on how finances are invested and distributed by states and private entities with regard to the development of technology are to be regarded as second-order economic agents as the work they do ensures that finances are not expended in manner that may prove to be detrimental.

4.2.6. Second-order scientific agents

A) Agent name: Cybersecurity for Democracy

Established: 2021

Nature of work: “Cybersecurity for Democracy is a research-based, nonpartisan, and independent effort to expose online threats to our social fabric – and recommend how to counter them. We are

part of the Center for Cybersecurity at the NYU Tandon School of Engineering” (cybersecurityfordemocracy, n.d.). The organisation analyses the extent to which online communication and information sharing platforms can be used to spread misinformation. The organisation seeks to highlight the vulnerabilities that makes these platforms susceptible to “misinformation attacks” and then help with the development of “mitigation strategies to improve online security”. The organisation analyses widely used platforms such as Facebook, Twitter and YouTube as they have found that these platforms are used extensively to spread misinformation and weaken democracy (cybersecurityfordemocracy, n.d.). An important part of the organisation's work is that it advocates for data “transparency and standardisation” to allow for the auditing of online platforms. In line with democratic norms and standards, the data collected by the organisation is shared with others to provide further feedback and analysis.

As an actor that is focused on the protection of democracy, truth and transparency, Cybersecurity for Democracy ensures the protection of human rights and the realisation of human rights that relate to access to information. The work is important to democratic societies as cyberspace play an important in the dissemination of information and has made it easier for various actors to spread information. Through its actions, the organisation also ensure protection from state overreach which allows for freedom of association and prevents the censoring of the internet. The work of the organisation ensures equal security for all and avoids creating a burden of insecurity for one group while trying to secure another.

This chapter will now proceed to provide an analysis of cybersecurity actions carried out by the listed cybersecurity agents and show how their actions contribute to the creation of a more secure cyberspace through actors' actions. The analysis will highlight the relationships the actors share with other agencies involved in cybersecurity.

4.3. Threat analysis and response

A) Distributed Denial of Service Attack (DDoS)

“DDoS attacks are cyber-attacks on specific servers or network with the intended purpose of disrupting that network or server’s normal operation” (Agrawal, 2019: 2). Such attacks on important public and private services can result in a range of operational issues for the affected organisation and also negatively impact those who rely on the services provided by the affected organisation. DDoS attacks work by overwhelming systems by submitting more requests than the system is designed to handle. The influx of requests hampers the system’s ability to respond to legitimate requests. These attacks not only affect the immediate operation of the system but also negatively affect future operations as the system has to be taken offline which can lead to the exploitation of other vulnerabilities and also affect the organisation’s position within the market.

Various efforts have been made to protect infrastructure against such attacks and also to minimise the impact should systems be breached. “Classification algorithms have been used in many studies and aimed to detect and solve the DDoS attacks” (Agrawal, 2019: 2). The development of algorithms and machine learning have allowed for automation and limiting human intervention for computers to learn more about the patterns of such attacks, how to block and how to resolve them. Various algorithms have been developed such as Random Forest algorithms, Apache Spark and Multi-Layer Perception (MLP). Despite the strides that have been made, many companies and organisations still fall victim to DDoS attacks. According to Arbor Networks, a network security and monitoring company, 124,000 DDoS attacks were tracked each week between January 2015 and June 2016. “Furthermore, 274 of the attacks observed in the first half of 2016 reached over 100 Gbps (as compared to 223 in all of 2015), while 46 attacks registered above 200 Gbps (as compared to 16 in 2015)” (Bisson, 2016).

As previously mentioned, attacks stifle the standard operation of the services with wide-ranging effects. This is why there have been multiple efforts from private and public first-order agents to develop systems and software that can be used to prevent such attacks. There have been investments by private investment companies such as Sequoia Capital and others in cybersecurity companies and network monitoring companies. Other companies have also received funding and support from accelerators such as Y Combinator. Above this, there has also been work carried out by government agencies such as USCYBERCOM which helps with the protection of infrastructure and improvement of capabilities. These relationships and cooperation efforts help promote the protection of the country's cyber domain.

B) Ransomware attacks

Ransomware attacks work by encrypting the users' information making it inaccessible and demanding a ransom from the user for the information to be decrypted or for the user to receive instructions on how to decrypt the information. Tandon and Nayya (2019: 2) define ransomware attacks as a “malicious class of software that utilises encryption as a method to implement an attack on system availability. The victim’s data remains encrypted and held captive by the attacker until the ransom demand is met”. Not all ransomware attacks are the same as these attacks fall into two major categories in the form of crypto-ransomware and locking ransomware. “Crypto ransomware is characterized by its ability to encrypt files, thereby immobilizing victims who are thus powerless without the decryption key. While locking ransomware locks and/or disables some services in the victim’s machine” (Alqahtani and Sheldon, 2022: 1).

There are different ways in which victims can have the ransomware downloaded onto their computers. These include connecting to insecure networks, using computer accessories that have been compromised or being the victim of a phishing attack. One of the most common ways in which ransomware is downloaded onto computers is through visiting websites or through email attachments.

The prevalence of these attacks, especially after the Covid-19 pandemic which has led to more

people being reliant on their computers, has led to increased efforts to make internet users more aware of the potential dangers they face online (Alqahtani and Sheldon, 2022). This is important not only for user safety but also for the protection of public and private systems from external threats as most ransomware can be distributed on company servers and networks and can be programmed to avoid detection by firewalls and antivirus software.

As recently seen in the USA, ransomware attacks can negatively affect millions of people and result in excessive ransom payments. Two attacks in 2021 affected fuel supply and food processing. Writing about the attacks, Alqahtani and Sheldon (2022: 1), write “the attack against Colonial Pipelines that took place in May 2021 is an infamous ransomware incident that disrupted the operations of the major fuel supply chain in 17 states including Washington. The company had no choice but to pay around USD 4.4 million. Within the same period, another attack targeted JBS, the world’s largest meat processor”. These two attacks demonstrate how an absence of an effective cybersecurity strategy can lead to a widespread disturbance outside of the systems considered to be the most important such as banking, electricity grids and healthcare service.

Due to the impact of the attacks, the US DoJ in partnership with other government agencies had to work with private sector actors to regain control of the affected systems. Other government agencies such as the Department of Homeland Security (DHS) and the FBI Cyber Division were involved as the two attacks were categorised as terrorist attacks by the DoJ. The relationship and actions of first-order helped in the resumption of standard operations. The magnitude of the matter has required the involvement of the NSTC to help the government in its cybersecurity strategy and policy. The actions of cyber defence and policy help in securing the nation's cyber infrastructure.

C) Cybersecurity and democracy

Cyberspace has become an important part of all societies as it plays an important in the functioning of many important services that are used daily. The raise in reliance on cyberspace for many

societal functions has led to many nations working to have offensive and defensive cyber capabilities. These efforts have led to the creation of various legislation, cooperative agreements and the assigning of certain cybersecurity duties to the militaries of countries through the establishment of cybersecurity wings as previously demonstrated in the case of the USA. The defensive duties are assigned to militaries as they are seen as affecting "sovereign states and their critical assets across territorial jurisdictions" (Simola and Lehto, 2020: 392). With cybersecurity being an emerging field in security studies, the initial conception of security has followed that which was seen in conventional warfare of the state being the main referent object that requires protection.

With more research being conducted and more information becoming available, questions have been raised about the cyber capabilities with which the military is entrusted. The questions arise due to the shared use of cyberspace with software and hardware use not being easily delineated between civilians and the military. Simola and Lehto (2020: 392-393) capture this concern in writing, "the problem is that the armed forces, intelligence and law enforcement agencies tend to operate under 'limited public accountability, oversight, and transparency'". Allowing the military to possess all critical cyber capabilities or have the ability to potentially control companies that own and manage ICT creates concerns over a free and fair internet void of censorship and user limitations.

As such, it is important for there to be secondary non-partisan and unbiased organisations that monitor the government's efforts to secure cyberspace and the methods with which it goes about securing the cyber domain. Organisations such as Cybersecurity for Democracy from the New York University (NYU) Center for Cybersecurity are important to discourse on legislation and international cooperation as they conduct research on cyber governance which analyses the development and enforcement of policies and legislation. The organisation also seeks to "identify the appropriate roles and obligations of various stakeholders—including private companies and government agencies. This includes issues of technical capacity, the regulatory environment, and commercial incentives" (NYU Center for Cyber Security, n.d). The organisation also researches cybercrime, national cyber strategies, digital forensics, software and system security, supply chain

security and security of cyber-physical systems.

The work and relationships second-order agents have with one another and first-order agents are important not only to ensuring that human norms and values are adhered to, but they also assist in supplementing work being carried out by various agencies which can be used to avoid shortcomings and address other issues and consequences the organisation might have not been aware of.

With cyberspace being an international common good, threats can arise from any region. As such, countries need to work together through public and private partnerships to guard against various threats including misinformation and disinformation. This is why first-order political agents such as the US DoJ have been working with the governments of developing nations and their cyberspace non-governmental organisations (NGOs) which are second-order political and scientific agents to help them create legislation, strategies, research and technical training. For example, the "US-Chile Executive Cyber Consultation mechanism focused on bilateral cooperation, collaboration, the protection of critical infrastructure, incident response, data security, information and communication technology procurement, and military and law enforcement cooperation" (Simola and Lehto, 2020: 397).

There has also been participation in cyber governance by first-order technological actors such as Microsoft which has established the 'Security Policy for a Connected World' which is an initiative that is geared toward helping organisations, nations and regions protect themselves against "new and emerging threats" through public policy and research based on four "broad themes of concern to policymakers" which are cybersecurity policy and resilience, cloud security and assurance, digital Geneva Convention and cybercrime legislation and strategy (Microsoft, n.d.).

Relationships between key actors affect the realisation of cybersecurity as the key actors shape research and development, guide discourse and also influence the extent to which domestic and international cooperation takes place. The creation of a typology of cybersecurity agents helps in

understanding the roles and positions different cybersecurity actors occupy within a given society. The typology's categorisation aids in the analysis of shortcomings of current methods and allows for systematic future planning to help improve cybersecurity. As shown in the provided case examples, there are multiple players involved in cyber security incidents which require cooperation between private and public first-order and second-order agents. First-order agents play an important role in defining and shaping cybersecurity through legislation, policing, hardware and software development, research and investment. Second-order agents play an important role in the cyberspace domain as they ensure that all actions carried out by first-order agents are in line with established norms and human rights. These actions help ensure that not only is cybersecurity realised in the form of infrastructure protection and user safety, but it also guarantees that the provided cybersecurity does not create a burden of insecurity for parts of society while securing another as stated by Loader and Walker.

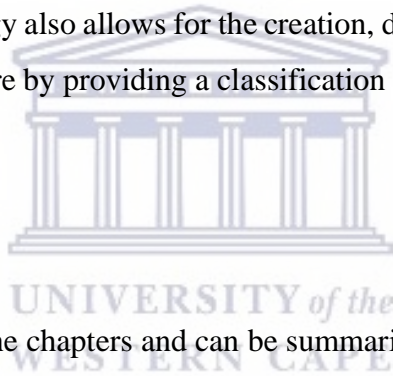
4.4. Conclusion

The chapter has provided a populated illustration of the typology of cybersecurity agents and has shown how the relationships and actions of various actors contribute to the realisation of a secure cyberspace. The six categories under which the cybersecurity agents can be classified were provided along with an outline of each category and examples for illustrative purposes. The examples were selected to show how the categorisation criteria can be employed for agent analysis by using the typology that was developed in chapter 3. The next chapter will present the conclusion of the thesis and provide areas for future research.

Chapter 5: Conclusion

5.1. Introduction

The final chapter provides a succinct summary of the thesis and avenues for further research. The thesis set out to develop a typology that can be used to analyse cybersecurity provision by mapping cybersecurity agents. The development of such typologies and other structures are important to facilitate the safe, equal and shared growth of cyberspace. Such a typology has policy relevance in that it can identify repetition and overlapping of duties, tasks or gaps in cybersecurity architecture at various levels and spheres of society. The typology can also be used to inspire and inform structured and progressive dialogue and cooperation among different actors from different cybersecurity sectors. The typology also allows for the creation, development and improvement of existing agencies and infrastructure by providing a classification schema for cybersecurity agents.



5.2. Summary of argument

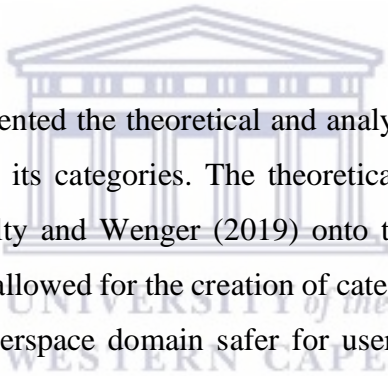
The argument unfolded through the chapters and can be summarised as follows:

Chapter 1: The first chapter of the thesis introduced the nature of the problem investigated. The chapter also provided the research question, sub-questions) and the research aim. The chapter provided the background to the problem and also presented the problem statement. The first chapter stated the importance of the research and stated the methodology that was used in the development of the typology. The delimitations of the study were presented as well.

Chapter 2: The second chapter of the thesis presented the broad and expansive history of cyberspace. The chapter detailed the development of the internet, its software, hardware and subsequent developments due to the growth in the availability and access to cyberspace infrastructure and related technologies. The chapter also analysed insecurities which lie in

cyberspace and affect all users. The chapter then explained how the improvement of mobile phone technology led to a growth in the number of internet users.

A new field of growth presented in the chapter was the Internet of Things which is linked to the improvement of mobile phone technology. Presenting the history of cyberspace and resulting insecurities was important for two reasons towards the development of the typology. First, the chapter demonstrated the multiplicity of the issues that lie in cyberspace and showed how different actors play differing roles in cyberspace. Second, the chapter played an important role towards the development of the typology as it demonstrated the rapid pace at which cyberspace technology develops. The speeds at which the technology develops are important to consider as laws are required to regulate new technologies.



Chapter 3: The third chapter presented the theoretical and analytical framework that guided the development of the typology and its categories. The theoretical framework was developed by superimposing the work of Cavelti and Wenger (2019) onto the work of Loader and Walker (2007). The two works combined allowed for the creation of categories to classify actors based on whether they are making the cyberspace domain safer for users or safeguarding users against security measures that may impact on their human rights. As previously stated, the chapter was important in the development of the typology as it informed the classification categories that were used in the populated matrix in chapter four.

Chapter 4: The fourth chapter presented the six-type categorisation of the agents and populated the matrix diagram to illustrate the typology. The chapter provided information regarding the roles the actors from different spheres play with regards to the civilising of the cyber domain and the civilising of cybersecurity provision. The chapter also provided an analysis of the impact the relationships and actions of cybersecurity actors have on the realisation of a secure cyberspace.

5.3. Limitations

The study faced challenges in its development. The stud had initially intended to analyse the South African cybersecurity landscape. The analysis required the interviewing of South African cybersecurity agents working in various sectors. Due to Covid-19 and difficulty recruiting interviewees, the initial intent of analysing South Africa’s cybersecurity landscape was stymied and the methodology could not be applied. As such, the study adapted the research methodology to a desktop study and illustrated the typology developed in this thesis by using examples from different states. These examples were traced and researched online.

5.4. Areas for future research

The research provides the foundation for several avenues for future research

5.4.1. Domestic application

Investigating ways in which the typology could be refined by distinguishing between domestic and international cybersecurity agents of each order and in each sector. This is an important area of investigation as the agents involved in the provision of cybersecurity and adherence to human rights and democratic values differ based on whether the stage is domestic or international. I Being able to map the agents across these two stages will allow for a well-informed separation of roles and responsibilities as well as how cybersecurity norms develop and spread from national to international environments and national again. This would also inform how nations apply regional and international treaties to which they are signatories in their countries based on their constitutions.

5.4.2. Case study application

An investigation that seeks to apply the typology to a nation's cybersecurity architecture case study in order to understand and outline the overlaps and shortcomings in a nation’s cybersecurity

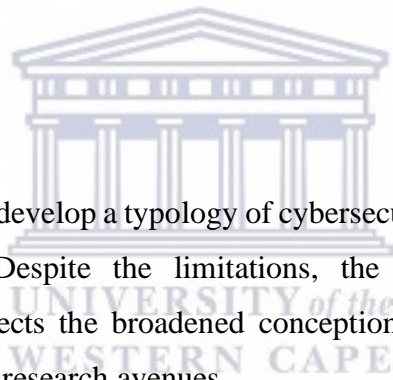
architecture is an area worthy of future research. Such an investigation would allow for the realisation of required policies, required actions, possible domestic partnerships, possible international partnerships and the most urgent actions required to ensure cybersecurity.

5.4.3. Comparative studies

The typology can also be used to compare and contrast cybersecurity agents in different countries or regions. Such comparisons can be used to further cooperation amongst states, e.g., BRICS, NATO or African Union countries can identify where the strengths and weaknesses of each country are in the alliance are which can be used to better inform cooperation and development.

5.5. Conclusion

In conclusion, the study set out to develop a typology of cybersecurity agents that has practical use to map cybersecurity agents. Despite the limitations, the study collated knowledge on cybersecurity in a way that respects the broadened conception of security, while providing a foundation for a number of future research avenues.



6. Reference List

Abbate, J., 2000. *Inventing the internet*. MIT press.

atih.responsibletechguide.com. (n.d.). About 3 —. [online] Available at: <https://atih.responsibletechguide.com/about> [Accessed 20 Nov. 2021].

Agrawal, N. and Tapaswi, S., 2019. Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, 21(4), pp.3769-3795.

Alemneh, D.G. and Hastings, S.K., 2006. Developing the ICT infrastructure for Africa: Overview of barriers to harnessing the full power of the Internet. *Journal of Education for Library and Information Science*, pp.4-16.

Alqahtani, A. and Sheldon, F.T., 2022. A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. *Sensors*, 22(5), p.1837.

Beranek, L.L., 2007. Who really invented the internet?. *Sound and Vibration*, 41(1), pp.6-15.

Bickerstaff, S., 1999. Shackles on the giant: how the federal government created microsoft, personal computers, and the internet. *Tex. L. Rev.*, 78, p.1.

Bisson, D. (2016). <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-ddos-attacks-2016>.

Bryant, R., 2001. What kind of space is cyberspace. *Minerva-An Internet journal of philosophy*, 5(2001), pp.138-1.

Buzan, B., Wæver, O., Wæver, O. and De Wilde, J., 1998. *Security: A new framework for analysis*. Lynne Rienner Publishers.

Calderaro, A. and Craig, A.J., 2020. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), pp.917-938.

Cerf, V. and Aboba, B., 1993. How the Internet came to be. *The On-line User's Encyclopedia: Bulletin Boards and Beyond*. Reading, Massachusetts: Addison-Wesley.

Chandler, D., 1995. Technological or media determinism.

Chandler, D., 2010. The uncritical critique of 'liberal peace'. *Review of international studies*, 36(S1), pp.137-155.

Chiang, M.F., Cole, R.G., Gupta, S., Kaiser, G.E. and Starren, J.B., 2005. Computer and world wide web accessibility by visually disabled patients: Problems and solutions. *Survey of ophthalmology*, 50(4), pp.394-405.

Chibucos, T.R., Leite, R.W. and Weis, D.L. eds., 2005. *Readings in family theory*. Sage.

Cross, C., 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), pp.187-204.

CyberBRICS. (2019). *About us*. [online] Available at: <https://cyberbrics.info/about-us/> [Accessed 27 Sep. 2021].

Cybercom.mil. (2017). *Mission and Vision*. [online] Available at: <https://www.cybercom.mil/About/Mission-and-Vision/>.

cybersecurityfordemocracy.org. (n.d.). *Cybersecurity for Democracy*. [online] Available at: <https://cybersecurityfordemocracy.org/about> [Accessed 22 Nov. 2021].

defenceWeb. (2019). Armscor cybersecurity unit up and operational. [online] Available at: <https://www.defenceweb.co.za/cyber-defence/armscor-cybersecurity-unit-up-and-operational/> [Accessed 22 Nov. 2021].

Dhamija, R., Tygar, J.D. and Hearst, M., 2006, April. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590).

Dsouza, Z., 2017. Are cyber security incident response teams (CSIRTs) redundant or can they be relevant to international cyber security. *Fed. Comm. LJ*, 69, p.201.

Dunkels, A., 2003, May. Full TCP/IP for 8-bit architectures. In *Proceedings of the 1st international conference on Mobile systems, applications and services* (pp. 85-98).

Dunn Cavelt, M. and Wenger, A., 2020. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), pp.5-32.

Du Toit, R., Hadebe, P.N. and Mphatheni, M., 2018. Public perceptions of cybersecurity: a South African context. *Acta Criminologica: African Journal of Criminology & Victimology*, 31(3), pp.111-131.

Gañán, C.H., Ciere, M. and van Eeten, M., 2017, October. Beyond the pretty penny: The economic impact of cybercrime. In Proceedings of the 2017 new security paradigms workshop (pp. 35-45).

Gazet, A., 2010. Comparative analysis of various ransomware virii. *Journal in computer virology*, 6(1), pp.77-90.

Glaser, C.L., 1997. The security dilemma revisited. *World politics*, 50(1), pp.171-201.

Grieco, J.M., 1988. Anarchy and the limits of cooperation: a realist critique of the newest liberal institutionalism. *International organization*, 42(3), pp.485-507.

Guzzini, S., 2004. The enduring dilemmas of realism in international relations. *European Journal of International Relations*, 10(4), pp.533-568.

Gwartney, J. and Stroup, R. (1998). TEN KEY ELEMENTS OF ECONOMICS. Available at: <https://www.heartland.org/publications-resources/publications/ten-key-elements-of-economics> [Accessed 20 Sep. 2021].

Harvard Business Review. (2014). *The Sectors Where the Internet of Things Really Matters*. [online] Available at: <https://hbr.org/2014/10/the-sectors-where-the-internet-of-things-really-matters>.

Hawker, N., 2005. Internet browsers. *Network Access, Regulation and Antitrust*, p.177.

Heiss, A., & Johnson &, T. (2019). Liberal Institutionalism. In A. Heiss & T. Johnson, *International Organization and Global Governance, 2nd ed., ed.* (2nd ed., pp. 1-21).

Hemer, J., 2011. A snapshot on crowdfunding (No. R2/2011). *Arbeitspapiere Unternehmen und Region*.

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

Hills, J., 2006. What's new? War, censorship and global transmission: from the telegraph to the internet. *International Communication Gazette*, 68(3), pp.195-216.

Home.cern. (2019). The birth of the Web | CERN. [online] Available at: <https://home.cern/science/computing/birth-web>.

Hong, J., 2012. The state of phishing attacks. *Communications of the ACM*, 55(1), pp.74-81.

Hoover, G. (2020). Most Valuable Companies: The Last 25 Years. [online] Business History - The American Business History Center. Available at: <https://americanbusinesshistory.org/most-valuable-companies-the-last-25-years>.

Islam, R., Islam, R. and Mazumder, T., 2010. Mobile application and its global impact. *International Journal of Engineering & Technology (IJEST)*, 10(6), pp.72-78. D

ITU (2019). *About ITU*. [online] Itu.int. Available at: <https://www.itu.int/en/about/Pages/default.aspx>.

Jordan, T. and Taylor, P., 2004. *Hactivism and cyberwars: Rebels with a cause?*. Routledge.

Justice.gov. (2018). *About DOJ*. [online] Available at: <https://www.justice.gov/about>.

Keohane, R.O., 2012. Twenty years of institutional liberalism. *International Relations*, 26(2), pp.125-138.

Keohane, R.O. and Martin, L.L., 1995. The promise of institutionalist theory. *International security*, 20(1), pp.39-51.

Kharpal, A. (2021). *China spending on research and development to rise 7% per year in push for major tech breakthroughs*. [online] CNBC. Available at: <https://www.cnbc.com/2021/03/05/china-to-boost-research-and-development-spend-in-push-for-tech-breakthroughs.html> [Accessed 16 Jun. 2021].

Koba, M. (2011). *BRICS: CNBC Explains*. [online] CNBC. Available at: <https://www.cnbc.com/id/44006382>.

Krause, C.A. and Pazicky, L.A., 2008. An un-Standard condition: restricting Internet use as a condition of supervised release. *Federal Sentencing Reporter*, 20(3), pp.201-205.

Laskar, M., 2013. Summary of social contract theory by Hobbes, Locke and Rousseau. *Locke and Rousseau (April 4, 2013)*.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. and Wolff, S., 2009. A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, 39(5), pp.22-31.

Leiter, B., 2001. Classical realism. *Philosophical Issues*, 11, pp.244-267.

Li, S., Da Xu, L. and Zhao, S., 2015. The internet of things: a survey. *Information Systems Frontiers*, 17(2), pp.243-259.

Libicki, M.C., 2016. Is there a cybersecurity dilemma?. *The Cyber Defense Review*, 1(1), pp.129-140.

Loader, I. and Walker, N., 2007. *Civilizing security*. Cambridge University Press.

London: London: Routledge. Retrieved from <https://www.andrewheiss.com/files/research/2018-johnson-heiss-liberal-institutionalism.pdf>

Lufkin, B. (2020). *The curious origins of online shopping*. [online] BBC. Available at: <https://www.bbc.com/worklife/article/20200722-the-curious-origins-of-online-shopping>.

Maryska, M., Doucek, P. and Kunstova, R., 2012. The importance of ICT sector and ICT university education for the economic development. *Procedia-Social and Behavioral Sciences*, 55, pp.1060-1068.

Miller, C., 2017. What is responsible technology, anyway? [online] www.medium.com. Available at: <https://medium.com/doteveryone/what-is-responsible-technology-anyway-8b4a86f3c316> [Accessed 20 Nov. 2021].

Mockapetris, P. and Dunlap, K.J., 1988, August. Development of the domain name system. In *Symposium proceedings on Communications architectures and protocols* (pp. 123-133).

Molla, A. and Licker, P.S., 2001. E-commerce systems success: An attempt to extend and respecify the Delone and MacLean model of IS success. *J. Electron. Commer. Res.*, 2(4), pp.131-141.

Morris, J.J. and Alam, P., 2012. Value relevance and the dot-com bubble of the 1990s. *The Quarterly Review of Economics and Finance*, 52(2), pp.243-255.

Nuruzzaman, M., 2008. Liberal institutionalism and international cooperation after 11 September 2001. *International Studies*, 45(3), pp.193-213

NYU Center for Cyber Security. (n.d.). Research. [online] Available at: <https://cyber.nyu.edu/research/> [Accessed 23 Jun. 2022].

ONS.gov.uk. (2017). *Government expenditure on science, engineering and technology, UK - Office for National Statistics*. [online] Available at: <https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgovernmentexpenditureonscienceengineeringandtechnology/2017>.

PK, F.A., 1984. What is Artificial Intelligence?. "Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do", p.65.

Pretorius, J., 2008. The technological culture of war. *Bulletin of Science, Technology & Society*, 28(4), pp.299-305.

Reiter, B., 2013. The epistemology and methodology of exploratory social science research: Crossing Popper with Marcuse.

Rid, T. and McBurney, P., 2012. Cyber-weapons. *the RUSI Journal*, 157(1), pp.6-13.

Republic of South Africa (2016). CYBERCRIMES AND CYBERSECURITY BILL. Available at: <https://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf> [Accessed 10 Jul. 2021].

Roberts, L.G., 1978. The evolution of packet switching. *Proceedings of the IEEE*, 66(11), pp.1307-1313.

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. *Future Internet*, 11(4), p.89.

Satapathy, A. and Livingston, J., 2016. A Comprehensive Survey on SSL/TLS and their Vulnerabilities. *International Journal of Computer Applications*, 153(5), pp.31-38.

Shane, S., 2002. Selling university technology: Patterns from MIT. *Management science*, 48(1), pp.122-137.

Simola, J. and Lehto, M., 2020. National Cyber Threat Prevention Mechanism as a part of the E-EWS. In *The proceedings of the... international conference on cyber warfare and security*. Academic Conferences International.

Snyders, D. (n.d.). *All the companies Naspers owns*. [online] Available at: <https://mybroadband.co.za/news/business/404845-all-the-companies-naspers-owns.html>.

Stein, A.A., 2008. Neoliberal institutionalism. *The Oxford handbook of international relations*, pp.201-221.

Subramanya, S.R. and Lakshminarasimhan, N., 2001. Computer viruses. *IEEE potentials*, 20(4), pp.16-19. A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook

Sutherland, E., 2017. Governance of cybersecurity—the case of South Africa. *The African Journal of Information and Communication*, 20, pp.83-112.

The White House. 2022. *National Science and Technology Council (NSTC) | The White House*. [online] Available at: <<https://www.whitehouse.gov/ostp/nstc/>> [Accessed 19 June 2022].

Uma, M. and Padmavathi, G., 2013. A Survey on Various Cyber Attacks and their Classification. *Int. J. Netw. Secur.*, 15(5), pp.390-396.

United States Department of State. (n.d.). *Digital Connectivity and Cybersecurity Partnership*. [online] Available at: <https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/> [Accessed 26 Sep. 2021].

Usman, A. and Shami, S.H., 2013. Evolution of communication technologies for smart grid applications. *Renewable and Sustainable Energy Reviews*, 19, pp.191-199.

Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, 38, pp.97-102.

West, D.M., 2015. Digital divide: Improving Internet access in the developing world through affordable services and diverse content. *Center for Technology Innovation at Brookings*, pp.1-30.

Williams, P.D. ed., 2012. *Security Studies: an introduction*. Routledge.

Wortmann, F. and Flüchter, K., 2015. Internet of things. *Business & Information Systems Engineering*, 57(3), pp.221-224.

www.digitalcitizensalliance.org. (n.d.). *About the Digital Citizens Alliance*. [online] Available at: <https://www.digitalcitizensalliance.org/about/about-the-digital-citizens-alliance/> [Accessed 3 Oct. 2021].

www.microsoft.com. (n.d.). Cybersecurity Framework & Policies | Microsoft Cybersecurity. [online] Available at: <https://www.microsoft.com/en-us/cybersecurity/?activetab=cyber%3aprimar2>.

www.ycombinator.com. (n.d.). About Y Combinator. [online] Available at: <https://www.ycombinator.com/about/>.

Zamora, J., 2020, June. 28 Days Later: New Internet Users in Brazil and India Try a Lite Smartphone for a Month. In Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies (pp. 53-64).