BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SOCIAL SCIENCES AND HUMANITIES

DEPARTMENT OF PEACE AND GOVERNANCE

CYBER WARFARE AS A NEW THREAT TO SECURITY POLICY: A RUSSIAN FOREIGN POLICY PERSPECTIVE.

BY

B1747871

A DISSERTATION SUBMITTED IN PARTIAL FULFULMENT FOR THE REQUIREMENTS OF THE MASTER OF SCIENCE DEGREE IN INTERNATIONAL RELATIONS

SUPERVISOR: DR MBANJE

BINDURA, ZIMBABWE 2019

DECLARATION

I Mugwira Edwin hereby declare that the work reported in this dissertation is my original work and it has never been submitted for award of any certificate, diploma or degree in this or any other University or institution.

Signature …… Date ……

APPROVAL

This dissertation/thesis entitled “Cyber warfare as a new threat to security policy: A Russian foreign policy perspective..” by Mugwira Edwin meets the regulations governing the award of the degree of Master Of Science Degree In International Relations of the Bindura University Of Science Education, and is approved for its contribution to knowledge and literal presentation.

Supervisor …….

Date ……

DEDICATION

This dissertation is dedicated to my lovely wife for the support and encouragement she accorded me during the taxing period of getting this study done.

ACKNOWLEDGEMENTS

A number of people contributed in one way or the other to this piece of work. First and foremost, I would like to express my sincere appreciation to Dr Bowden Mbanje for the supervision provided during the course of the whole study. I would also want to thank all my lecturers and the entire staff in the Department of Peace and Governance for their contribution to my successful completion of this course.

My sincere gratitude is also due to all my classmates from the 2018-2019 Masters in International Relations class for all the support and companionship. To Dr Alexander Maune thank you for the support, encouragement and constructive criticism rendered during the course of this study.

ABBREVIATIONS AND ACRONYMS

ARPANET	Advanced Research Projects Agency Network
CIS	Commonwealth of Independent States
CNA	Computer Network Attacks
CNE	Computer Network Exploitation
DDoS	Distributed Denial-of-Service
ECM	Electronic Counter Measures
ECCM	Electronic Counter-Counter Measures
ICT	Information and Communication Technology
ISP	Internet Service Providers
NASA	National Aeronautics and Space Administration
NPT	Nuclear Non-Proliferation Treaty
USA	United States of America
USSR	Union of the Soviet Socialist Republic

Table of Contents

ABSTRACT

Cybersecurity is one of the most recent and unique national security issues of the twenty-first century. The world has witnessed a significant number of cyber-attacks perpetrated by various actors in the international system for various objectives. Therefore this study seeks to understand the Russian foreign policy regarding this new domain of international relations. The Russian approach to cyber warfare, both theoretical and practical underpinnings, was to be examined. The study discussed the conceptual framework that underlines the principle of Russia`s cyber warfare, national and foreign policy. The research was informed by the qualitative research methodology which gives respondents an opportunity to completely air out their answers to questions asked. The study population composed of officials responsible for cybersecurity from the Ministry of Defence, Ministry of Foreign Affairs, Interpol Cyber Centre (Harare), academics, and renowned experts in the field of international relations.

The study is of value to strategic thinkers, politicians, academics in the field of International Relations and cybersecurity practitioners on how cyber vulnerabilities may compromise national security and may lead to catastrophic consequences. The research will enlighten authorities on the need for preparation for cyber-warfare in army-building. There is also an attempt by the study to bring to the fore nation-states, non-state actors who have also taken advantage of the vulnerability and interconnectivity of the cyberspace to inflict enormous damage to countries and societies.

The findings of the study show that the Russian foreign policy is heavily influenced by perceptions of threat and vulnerability. Russia's policy on information operations are shaped by many traditions. Russian leaders have long placed exceptional value on using information to manipulate their enemies. In light of these findings, the research recommends that states should set achievable long and short term actions to protect and defend critical ICT infrastructure.

CHAPTER ONE

INTRODUCTION

1.0 Background of the Study

The antagonistic relationship between Russia and the West in general and the United States of America (USA) in particular dates back to the Union of the Soviet Socialist Republic (USSR) era. The fall of the USSR and the consequent end of the Cold War era did not end this rivalry. It is against this background coupled with her desire to come back and influence decisions in the international system that underpins Russia`s foreign policy. According to Shevtsova (2002), President Vladimir Putin's tenure has seen Russia upgrading its national security, military and foreign policy to ensure that it progresses towards a multidirectional, balanced, and pragmatic external strategy. Kuchins (2005) explains that the current Russian foreign policy is largely rooted in its national interests. Kuchins (2005) further argues that, "Russia is striving for partnership with Washington not as a junior partner meekly accepting USA hegemony, but on an equal footing and to establish this equality; the Kremlin continues to strive to improve on its national security in terms of technological advancement."

Baldwin (1997) states that, "the concept of national security has traditionally included political independence and territorial integrity as values to be protected; but other values are sometimes added." In their quest to protect their territorial integrity, States focus more on their military preponderates or strength. Military strength allow countries to deter adversaries and also to defend themselves against aggression, while at the same time enabling state managers to pursue their national interests. These capabilities were much inclined to the protection of physical strategic entities. A state's military dominance was a sum total of its ground, air and sea prowess. Military capabilities or military effectiveness manifests itself from the resources that are made

available to military organizations by their governments. According to Paret (1989), “military power expresses and implements the power of the state in a variety of ways within and beyond the state borders, and is also one of the instruments with which political power is originally created and made permanent.” To Buzan et al (1998), “threats to national security are existential in nature impacting a nation on a strategic or political level.” Therefore, the state’s defense strategy takes into cognizant the nature of the threats that it faces.

In traditional warfare, army generals would seek to take and hold ground, use air forces to strike strategic targets and engage the enemy, while navies support land forces by conducting offshore attacks and cutting off lines of supply. In this information age, this approach to national security is changing due to new threats born out of technological advancement. A new facet of warfare is emerging which is asymmetric just as the scourge of terrorism. Technology has opened a space, cyberspace which states can manipulate to enhance their national security objectives.

National security concerns have been the driving force in determining a country’s foreign policy. The advent of globalisation has brought with it a new dimension of national security. With the interconnected nature of the world, brought about by information and communication technologies (ICT), states or countries are now more vulnerable than ever before in as far as their security is concerned. Technology brings with it a platform (cyberspace) which has become an indispensable part of a state, a society and the life of individuals. It is undeniable that states are now trying to maintain superiority over one another through technological advancement especially in cybersecurity. There are an increasing number of instances over the past four decades suggesting involvement of one nation in a cyber-attack toward another nation. Cyber-attack includes actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. Accordingly, Russia has been accused of using technology as a tool for espionage to further its foreign policy as it meddles in the internal affairs

of other states. The use of espionage via cyber operation is discreet, faster, and more scalable, than espionage by traditional means.

The Kremlin has been accused of using cyber warfare in Georgia, Ukraine and even on USA. The first known cyber-attacks initiated by Moscow against the USA military dates back to the late 1980s. By then, the Soviet Union, working in collaboration with East German's secret services, got assistance through West German's cyber proxies to undermine the USA security through cyber hacks. After realising the value and the low cost of remotely-conducted cyber intrusions, Moscow sought to overcome its 'cyber-laggard' status by developing a sophisticated arsenal of cyber espionage tools in the 1990s.This was despite the economic crisis affecting the country.

In 1996, Russia carried out successful cyber-attacks against USA in what came to be called the 'Moonlight Maze' case. According to Buchanan and Sulmeyer (2016:1),

> On October 7, 1996, well before such things were commonplace, the Colorado School of Mines suffered a digital break-in. The intruders gained access to a computer nicknamed 'Baby_Doe' in the school's Brown Building. To do this, they exploited vulnerabilities in the machine's Sun OS4 operating system. From there, they hopscotched to National Aeronautics and Space Administration (NASA), the National Oceanic and Atmospheric Administration, the U.S.A Navy and Air Force, and a long list of other computers spread across American universities and military installations. The operation went on for years, with the intruders collecting sensitive USA military and strategic information as they want".

Later investigations by the USA led the espionage cases to the work of Russian operators. Russia, however, is not the only country using technology to further its foreign policy. A number of cyber-attacks have been reported across the whole world and these include the following cases. In 1999, the cyber-attack between Pakistan and India were carried out

when the armed forces of both countries were engaged on the battlegrounds of Kargil. Around 2003, the Chinese hacked some USA servers for government. According to McGuinness (2017), "the Estonian government was a victim of cyber-attacks around April 2007; its IT infrastructure came under heavy attack resulting in the destruction of its strategic information centres including the country's websites and servers." The attack on Estonia was traced to Russia. Kyrgyz websites came under heavy attack in 2007 during an election campaign. Griggs (2008) asserts that, "the Georgian ICT infrastructure was heavily compromised in 2008 when Russia launched a cyber-attack along with a conventional attack on critical Georgian websites and servers disabling their communication and information services." In 2014 and 2015 intrusions were recorded targeting the USA State Department, the Pentagon, and the White House. The intrusions attracted enormous attention within the USA government. According to Schmidt and Sanger (2015), "the USA Secretary of Defense Ash Carter mentioned in a major speech in 2015 the importance of defending American networks. Therefore, this study seeks to determine the influence that cyber warfare has to national security policy."

1.1 Purpose of the Study

The study seeks to examine the Russian foreign policy on cyber warfare, through addressing its theoretical and practical underpinnings among other things.

1.2 Statement of the Problem

This study traces the evolution of cybersecurity approaches in Russia. The study is informed by the rising number of cyber invasions and operations across the whole world. The continuous increase in the number of cyber-attacks has become a problem both at national and individual levels. Russia because of its position in the geopolitical space has become a target of cyber-attacks especially from the West. Therefore, the study seeks to unpack Russia`s foreign policy with

regards to cybersecurity. The study further highlights the current cybersecurity debates taking place within Western security thinking.

1.3 Objectives of the Study

The broad objective of this study is to determine the influence of cyber warfare to security policy. In particular, the research attempts to:

- Analyse the Russian foreign policy vis-a vis national security.
- Examine the roots of Russian cyber security policy.
- Assess the response of state actors to Russian cyber-attacks.

1.4 Research Questions

- What is the Russian Foreign Policy from the perspective of national security?
- What are the origins of Russia's cyber security policy?
- How have states responded to Russia's cyber-attacks?

1.5 Assumptions of the Study

- Cyber warfare has become a new threat to national security.
- States are using cyber capabilities to further their national interests.
- Cybersecurity is a new form of deterrence.

1.6 Significance of the Study

This research will add to the body of knowledge on how cyber warfare has become a threat to national security. The increased use of cyber-attacks in recent years suggests that cyber warfare is becoming a new method of deterrence by super powers. It also seeks to add to the amplification of the voice calling for the crafting and adherence to international standards for governing the cyberspace. This gives rise to the question, whether current international laws can be applied to the cyber domain? Having in mind that at the core of these laws is governing of state actions

therefore, it follows that existing laws should be used as a guide. But it is the fluid nature of the cyber domain that makes it even difficult to effectively apply the laws. The dynamic nature of the domain does not help also.

It attempts to provide insights to strategic thinkers, politicians and cybersecurity practitioners on how cyber vulnerabilities may compromise national security and may lead to catastrophic consequences. Therefore, there is need to consider cyber warfare as a critical threat to security. The research will enlighten authorities on the need for preparation for cyber-warfare because of its importance in army-building. There is also an attempt by the study to bring to the fore non-state and nation-states actors who are taking advantage of the interconnectivity and vulnerability of the cyberspace effect cyber warfare on other countries.

Furthermore, the study seeks to help academics in the field of International Relations by providing valuable information on how far states can go in trying to pursue their national interests. Also insights are there for a comprehensive appreciation of geopolitics.

1.7 Delimitations of the Study

This study is subjected to two sets of delimitations. The first delimitation is of geographical coverage, concentrating the research on one representative state instead of analysing all other states engaging in cyber warfare although other states are refered to in the study. Secondly, the study was informed by the scope and time frame that was made available. The limitation relates to the depth of the analysis. So the study was limited to the security policy of Russia as informed by its foreign policy along cyber engagements with other states.

1.8 Limitations of the Study

The major limitation with the study was that often states and politicians, for reasons of state security or strategy, withhold certain information or alter it to protect or convey a certain image.

As a result the research risks being subjected to biases or subjective viewpoints as the majority of the participants of this research were politicians or diplomats who had a direct interest in the subject at hand. Furthermore, finances and accessibility to non-state actors' relevant to the subject of research proved to be a challenge to the researcher due to distance and other factors. Therefore, a maximum level of objectivity was demanded from the researcher in the review of literature and analysis processes.

1.9 Definition of Key Words

National Security

Frey et al. (1991) state that, "national security can imply all actions taken by a state's military unit to guarantee the state's protection from all actions that are designed to harm itself and the state. National security can also be defined as a national condition of a particular country perceived to be a state at which nations believe that there is no danger of military attack hence they can build up their nations and develop freely."

Cyber Power

According to Pontoon and Gill (1993:22), "power is the ability to get others to do what you wish assuming this is different from what they would otherwise have done, with the use of threat or sanctions if necessary." Couloumbis and Wolfe (1990:46) declare that, "power is the possession of strength derived from three elements, knowledge, military might and valour." Both definitions put into perspective of this study will help to define cyber power as the ability to use cyberspace in a positive way.

Cyber Warfare

Coughlan (2003:2) defines "cyber warfare as symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national

infrastructure and military systems. It requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advances on the part of the attacker. This is all done to achieve the state actor's security policy objectives."

Foreign Policy

Webber and Smith (2002) define foreign policy as, "composed of the goals sought, values set, decisions made and actions taken by states, and national governments acting on their behalf, in the context of the external relations of national societies." To Hill (2003), "foreign policy is the purposive action with a view towards promoting the interests of a single political community or state."

Padelford and Lincoln (1963) define foreign policy as, "the key element in the process by which a state translates its broadly conceived goals and interests into concrete courses of action to attain these objectives and pressure its interests."

Cyberspace

According to Wingfield (2000:17), "cyberspace is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, IT systems, and telecommunication infrastructures commonly referred to as the World Wide Web."

1.10 Organisation of the Study

The next chapter, Chapter Two dwells much on reviewing related literature critically looking at the findings in previous studies related to the study which will enable the researcher to identify the research gap. Chapter Three will focus on the methodology and design as it provides the operational framework. This Chapter will also highlight the master plan which reflects the

methods and procedures for collecting and analysing the needed information. In Chapter Four the researcher presents the collected and analysed data in different form. The last chapter will summarize, conclude and give recommendations. It will also provide recommendations that could be beneficial to various relevant groups and organisations that get benefits from this research project.

1.11 Conclusion

The above chapter provided the background, purpose, statement of the problem, objectives, assumptions, research questions, significance, delimitations, limitations as well as organisation of the study. Literature review, which is the next chapter scrutinises both empirical and theoretical literature on cyber warfare and security policy among others.

CHAPTER TWO

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

2.1 Introduction

A number of comprehensive books on cyber warfare have been written and entire issues of journals have been devoted to the topic. This chapter looks at the conceptual framework that underlines the principle of Russia`s cyber warfare, national and foreign policy. It is critical to examine literature on cyber warfare in relation to foreign policy so as to highlight the main issues in this study. The literature review should also help focus this study. The main issues to be examined relate to Russia`s national security narrative, information policy, how Russia is using information to advance her goals and cyber warfare perceptions. A snap evaluation of how Russia`s cyber-attack victims intend to or are responding to these attacks is also going to be carried out.

2.2 Conceptual Framework

The conceptual framework for this study is based on cybersecurity. The invention of Advanced Research Projects Agency Network (ARPANET) which later became the backbone of the World Wide Web in the early 1980s was safe and secure. This was so because everyone who had access to the system was known. The innovation focused more on interoperability and reliability in communication and control in case of emergencies. According to Winterfeld and Andress (2013), "trouble started with Robert Morris in the late 1980s when he released the first worm (a self-replicating piece of malware) and Clifford Stoll discovered Soviet Block spies stealing USA secrets via a mainframe at the University of California, Berkeley." These were quickly followed by a number of incidents that highlighted the security risks associated with this new innovation**.**

Technological developments have brought to the fore a virtual domain of international relations. A domain that has its own share of challenges, chief amongst them the issue of cybersecurity. This issue has made this cyber domain too important for national security. It is without doubt that the new domain is not there to bring order to the already chaotic terrain of international relations but rather cause more headaches. From a realist perspective, actors in the international system are seized with the ultimate objective of self-survival. According to Waltz (1979), "States in the international system serve their own interests by following a strict code of self-help due to absence of any authority above them." This idea of self-help in the international system and advances in technology is giving rise to the dilemma of cybersecurity.

Technology has transformed state governance. States are now depending heavily on technology in order to deliver their mandate. It is in the state's purview to offer critical social services to its citizenry and technology has become an enabler. Despite improving people's lives, this has exposed states to the vulnerabilities in the cyberspace hence the need to consider cybersecurity. It follows that all the necessary technological infrastructure becomes part of the state's strategic assets. As part of the national strategic assets, technological infrastructure joins the league of other national assets such as military hardware-tankers, fighter-jets and submarines that are there to preserve the state's wellbeing. Former USA President Barack Obama articulated the American view on cybersecurity in relation to national security objective. As reported by Whitehouse (2009), President Obama said, "From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."

To Myriam (2008), “the concept of cybersecurity gives attention to the concern of adequately securing government and military systems as well as addressing vulnerabilities in critical infrastructure.” Many scholars agree that the information revolution which is a direct result of technological advancement has changed how states view the concept of security. According to Softa (2008), “the information revolution is a global phenomenon that influences all aspects in society, such as international attitudes, the policy, the economy, the financial sector, science and culture. Information resources have become one of the most valuable national and international assets. At the same time there is a deep concern about the potential threats this progress can have on the international peace, stability, and security.” It is important to note that in this time and age states no longer take comfort in the traditional military power (sea, land, space) alone but seek also to have cyber power for survival.

2.3 Russia’s National Security Narrative

For the purposes of this study, the Russian national security issue will be traced from the Soviet Union era. National security according to Frey et al. (1991) implies, “all actions taken by a state’s military unit to guarantee the state’s protection from all actions that are designed to harm itself and the state.” Therefore states are susceptible to threats both domestic and foreign. This sense of insecurity amongst actors in the international system especially states have an influence on how they relate to each other. This general feeling of insecurity takes its toll also on Russia because of the lack of major natural boundaries to shield her. The conduct of these states as they interact becomes their foreign policies. This discussion will be guided by Hill (2003)’s definition of foreign policy which states that, “foreign policy is the purposive action with a view towards promoting the interests of a single political community or state.” From this definition it is clear that a state’s foreign policy has everything to do with national interests. Having said that and with the understanding of the international system, national security is one of many states interests.

Russia`s foreign policy is deeply persuaded by insights of danger and susceptibility. This situation has also not been made easy by its past foreign invasions and this has resulted in a national discourse of susceptibility and concern about foreign danger. Consequently, her grave security concerns have led her to prioritise a regional foreign policy. Consolidating relations with surrounding nations possibly exert her direct control over her neighbours enables her to create buffers for foreign invasion.

The present day Russia mirrors its foreign policy from her historical existence that exhibited a rich drapery of military prowess. Russia`s political and military thinking is grounded in Soviet Union past experience. The thinking is connected to the political prism through the ontology and epistemology of the Communist Party. A dark cloud of uncertainty befell Russia as a result of the collapse of the Soviet Union. Her influence in the region became questionable if not nonexistent. Moscow has always presumed that her leading position in the region was obvious and that would be seen by its neighbors and world at large. Even in her weakest position Russia did not lose her strategic culture which is rooted in its Eurasia setting, committed to its great power status and defined by persistent concerns over foreign intervention in its periphery.

A clear understanding of Russia's national interests will be of importance in evaluating the Russian foreign policy. Broadly, Russian interests may be summed up as, the desire to advance national defense, influence in the near abroad, vision to become a great power, non-interference in domestic affairs of other nations and the desire to restore her former glory. The course of the Russian foreign policy is influenced by a mix of internal causes and exogenous factors. Therefore it is incomplete to focus on Moscow's foreign policy ignoring its domestic social and political structure since foreign policy and domestic policy are two sides of the same coin. According to Light (2015), "several themes that embody Russia's main foreign policy interests and goals have

remained consistent since the birth of the post-soviet Russian state." Next sections will explore on the themes that drive her foreign policy.

2.3.1 Russian influence on the Commonwealth of Independent States

Russia's national security faces threats from quite a number of fronts. These threats have informed its foreign policy. The most persistent theme in Russia's foreign policy is her all-important relations with the Commonwealth of Independent States (CIS). These relations are sacrosanct to Russia. According to Lukyanov (2016), "Russia has historically considered Central Asia as its zone of influence, a chessboard where Russia would play to dominate." The plain geographical nature of Russia makes it vulnerable. This gives her a serious sense of insecurity which she tries to alleviate by creating buffer zones around herself making invasion almost impossible.

Although Russia is under no threat of any invasion, the westernization of the CIS is worrisome for the Kremlin who view it as a sophisticated invasion. Russia fears that such situation will result in western democracy views infiltrate into Russia to destabilize it. Kuchins and Zevelev (2012), highlights that, "the CIS, the former Soviet possessions, are so important to Russia's administration that it wants them under its influence because they represent a buffer to protect its core. Russian leaders, including the more moderated ones like Medvedev, have unfailingly considered the post-Soviet space as their primary foreign policy priority, a zone of privileged interests."

2.3.2 Russian opposition to North Atlantic Treaty Organisation's Eastward expansion

The frost relationship between Russia and USA brings this study to another theme on Moscow's foreign policy. Russia is aggressively against North Atlantic Treaty Organisation (NATO)'s eastward expansion. According to Cimbala (2013), "Russia's national security concepts and evolving expressions of military doctrine show its fears of surprise attack in the face of NATO

conventional military superiority, notwithstanding NATO's declaratory policy of nonhostility toward Russia." It is without doubt that the continuous eastward expansion of NATO is not healthy for Russia. And she has been persistently antagonized it. Lukyanov (2016) argues that, "following the collapse of the Soviet Union, the West started to spread democracy to the world in order to create a Western established international order. Since the Gulf War, the West has resorted to force, either through NATO or individual state actions, more and more often."

Sergei Karaganov (2011), a Russian political analyst holds that, "from a Russian perspective NATO has transformed from the purely defensive organization it was during the cold war, into an offensive organization: it is objectively difficult to contradict them. A more aggressive NATO has been incorporating countries that were former Soviet members (i.e. Baltic states and Poland) which have now become increasingly anti-Russian and that, most importantly, previously formed a buffer zone between NATO and Russia." A view echoed by Lukyanov (2016) as well. Having said that, it becomes apparent that NATO's expansion poses a serious threat to Russia`s national security. Specifically, if Ukraine were to join NATO, Russia would share a 2000 kilometers border with NATO, something it finds unacceptable.

Light (2015) argues that, "partly as a consequence of Western military interventions to bring regime change and the establishment of democracy, Russia has also always been a staunch defender of sovereignty, territorial integrity, and international law in general." Light (2015) further argues that, "as part of her foreign policy Russia has persistently defended its right to sovereignty and independence and has been critical of Western actions of interference in the domestic affairs of other states. It has also expressed a commitment to defend the norms of international law against unilateral or multilateral attempts on the part of other countries to change them." Appel (2008) agrees that, "the conduct of Russia in the arena of foreign affairs suggests that Russia is continuing to vacillate between its aspiration to keep the United States 'global

ambitions in check and the state of reality that requires it to bandwagon with the United States." President Putin's recent wars highlight a change in foreign policy. It is clear that Russia violated her commitment to non-interference.

2.3.3 Defense of sovereignty, territorial integrity, and international law.

Another threat to Russian national security which plays a role in informing her foreign policy is the deployment of ballistic missile defence systems, on the part of other countries, especially those closer to Russian borders. To Russia, such systems threaten global and regional stability as well as giving unfair advantage to countries embracing them. Russia feels that the West's meddling into politics is not different post-Soviet region support for democracy. This has resulted in the weakening of relations between Russia and the West.

2.4 Russian Cybersecurity Policy

2.4.1 Origins

The Russian perspective is grounded on its history and past grievances. Andrew and Mitrokhin (1999) argue that, "Russian national security policy begins with the perception that Russia lives in a constant state of siege that includes intelligence operations and the overall national security challenges posed by adversaries that are led by the United States." Andrew and Mitrokhin (1999) further argue that, "all authoritarian regimes, since they regard opposition as fundamentally illegitimate, tend to see their opponents engaged in subversive conspiracy." Russia has always believed that the conspiracies directed against her have been from foreign origin especially the West.

According to Vorobyov and Kiseljov (2013), " Information is now a species of weapon". When it comes to information, Russia believes it is an asset that can easily be converted into a powerful weapon against her enemies. During a television interview with NTV (a Russian free-to-air television channel) in Moscow in 2007, the then Russian Defense Minister Sergei Ivanov argued

that information technology has caused information to be used as a deadly weapon. Russia is using this weapon to carry out military actions in any threat of war without the use of military power. This has resulted in Russia taking all necessary steps in developing and improving the automatic control systems that is new and multi-purpose. Wirtz (2015) notes that, "Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives."

This was seen coming as the Russian military strategists had already foreseen that. According to Cimbala (2013), "Russian military planners suggested that, First, the battle for control over the electromagnetic spectrum will become more intense in the future, compared to the past: electronic countermeasures and counter-counter measures (ECM and ECCM, respectively) will figure more prominently in procurement and exercises for all modem armies, navies and air forces." Therefore, the use of technology to further Russian ambitions is premeditated.

Boot and Doran (2013) acknowledge that, "Russian conduct of both information war and cyber war builds on political warfare. Political warfare is the logical application of Clausewitz's doctrine in time of peace." Boot and Doran (2013) define political warfare in its broadest meaning, "as the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."

The former Soviet Union President Gorbachev's glasnost policy is partly blamed for the fall of the Soviet Union. The policy created an information gap which was manipulated to misinform and direct negative narratives towards the government of the day. This idea helps to explain the

current efforts by Russia in information and internet control. It is unsurprising that the 2000 Information Security Doctrine by Russia not only focuses on external but also on internal aspects, defining information security as "protection of national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state." The notion that information is regarded a danger that is deeply rooted in Russian foreign policy. Soldatov and Borogan (2015) point out that, "the Bolsheviks wanted newspapers to organize and mobilize the masses, not to inform them. Therefore the main purpose of Russia's information policy is to contribute to the stability of social and political developments within Russia and guarantee public support of official state policies." To Russians the information is the threat not the technologies used to manipulate the information. This is the explanation behind using terms such as information security and information policy.

2.4.2 Evolution

Historically, Russia has exhibited reliance on propaganda and disinformation strategies. Kenez (1995) states that, "Closer to the truth is that Russia has a long history of using information as a weapon – both in the context of mobilising its own population and in demonising foreign powers." Now she has managed to adapt these operations to the online environment. The concept of information/cybersecurity is viewed differently by the two main adversaries in this domain of international relations. The USA views cybersecurity as safeguarding disruptions in domestic technologies and unauthorized access as well as any kind of interference. Whereas the Kremlin focuses on information security, that is, protecting the nation's culture and knowledge, as well as guaranteeing the free flow of information. This has broadened the political and philosophical political meanings. Russia perceives technology as an important component in information security.

Technology has transformed the world bringing structural changes to the terrain of international relations. This globalisation drive has led to the formation of new centers of both political and economic power. This has motivated states to critically look on how to retain their areas of influence. As it becomes apparent that information can be weaponized, states are now investing in tools that keep them on guard in case an information war may be encountered. Thomas (2015) explains information war in its broadest sense as, " a conflict between two or more States in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents."

To Segal (2016), "the 2010 Military Doctrine of the Russian Federation describes information warfare as an instrument to achieve political objectives without the utilisation of military force and in combination with conventional means as a tool to create a favourable response from the world community." Clearly, Moscow is perfecting her tools in the information warfare front. Events of the Arab spring sent shocking waves to Moscow as it feared the level devastating effect of information. Soldatov and Borogan (2015) open up that, "it was not lost on Putin and his people that the events in Tunisia and Egypt were widely characterized as Facebook and Twitter revolutions. Putin and his entourage became worried that this time the United States had found a truly magic tool that could bring people to the streets without any organizing structure, the Internet."

Russia fine-tuned her information confrontation strategy in 2014 against Ukraine. The attack was quick and bloodlessly but reclaiming Crimea in the end and also keeping potentially intervening countries at bay. Iasiello (2017) reveals that, "after a series of military reforms resulting from the

2008 conflict with Georgia, Russia used information warfare operations more effectively in Crimea." According to Smith (2014), "Russia holds a broad concept of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems and propaganda. Computers are just among the many tools of information warfare, which is carried out 24 hours a day, seven days a week, in war and in peace. Russia's 2008 combined cyber and kinetic attack on Georgia was the first practical test of this doctrine." Furthermore, Smith (2014) argues that, "Russia finds value in manipulating the information space, particularly in an age where news can be easily accessed on demand through official and nonofficial outlets. Based on its successes in Crimea, Russia is outpacing its main adversary, the United States, by leveraging the information space to bolster its propaganda, messaging, and disinformation capabilities in support of geopolitical objectives."

2.5 How Russia is using information to advance her goals

As earlier on alluded to, Russia is amongst the top league in information warfare capabilities. The Russian aggression on the information front has led to confrontations with a number of states. Thomas (1998) refers to this as, "the Russian information confrontation theory, a theory covering a wide range of information offensive activities perpetrated by Russia and the conceptual understanding of Russian information operations stemming from cultural, ideological, historical, scientific, and philosophical viewpoints." The Russian philosophy in regards to information resonates with the popular saying "to inform is to influence." Thomas (1998) sees "the essence of the information confrontation theory focuses on constant information struggle between antagonistic parties. Reviewing the application of these principles in two well-known instances of Russian geopolitical involvement helps illustrate if and how Russian understanding of information confrontation has evolved. It also provides insight into the outcomes of such practices in the context of on-demand media coverage."

2.5.1 Previous Cyber Warfare Incidences

Different states and non-state actors have demonstrated capabilities of engaging in cyber warfare incidences for different reasons. This section of this paper will try to look closely on previously recorded attacks. Although the majority of the cases will be those orchestrated by Russia, some incidences instigated by other players will be discussed. It is of paramount importance that the analysis given for these attacks will try to bring to the fore, the main reasons for the attacks and the direct and indirect gains from the attacks. It is an undeniable fact that in recent history the occurrence of cyber-attacks has declined but this does not go for its impact.

Cases of Cyber-attacks by Russia

It has been widely claimed that Russia has championed many cyber-warfare attacks against other countries. The following listed attacks are attributed to Russian security services although Russia has vehemently denied them. Only those attacks of interest are listed here. Therefore, these may not be the only cyber-attacks carried out by Russia.

Estonia

The small nation of Estonia witnessed a series of cyberattacks on its ICT infrastructure. The most affected were websites for banks, media houses, and government departments which were attacked by enormous volumes of spam transmitted by botnets, DDoS attack. Due to this, many services were disrupted that relied on internet connectivity such as, email communication, mobile and online banking as well as media houses that failed to distribute news during the time.. The attacks reportedly came from Russian Internet Protocol (IP) addresses. Online instructions were in Russian and they were traced back to Russia. They were, however, no political signatures clearly link these attacks to Russia. The belief is that Russia was retaliating to a decision taken by

Estonian authorities. The Estonian government had taken a decision to relocate a monument to Soviet

Ukraine

Mazanec (2015) argues that, "around 2014, Russian cyber weapon called Snake was reported to have created havoc on Ukrainian government systems." According to Mazanec (2015), "the Snake tool kit began spreading into Ukrainian computer systems in 2010. It performed Computer Network Exploitation (CNE), as well as highly sophisticated Computer Network Attacks (CNA)." This cyber-attack occurred during the 2014 conflict between Russia and Ukraine over Russian invasion of Crimea. The attack resulted in a power outage. Russian hackers have a long history of participating in political and military conflicts in Eastern Europe and consistently carry out espionage operations around the world in support of Russian interests. According to Ghori and Unwala (2015), "Unlike the concurrent digital attacks and military border crossing in Georgia, cyberattacks against Crimea shut down the telecommunications infrastructure, disabled major Ukrainian websites, and jammed the mobile phones of key Ukrainian officials before Russian forces entered the peninsula on March 2, 2014."

Vijay et al. (2016) argue that, "the attack is believed to have been conducted by a Russian advanced persistent threat group called 'Sandworm' and occurred during an ongoing military and geopolitical conflict between Ukraine and Russia over Crimea." Vijay et al. (2016) summarize the intentions of this cyber-attack as, "compromising the network over email using BlackEnergy malware, harvesting user credentials, seizing the digital control system of the power plant by remotely switching off substations, disabling IT infrastructure components, destroying files that are stored on IT infrastructure using KillDisk malware and deploying a denial-of-service attack on the company call center." In this instance cyber warfare was used both as an offensive and

defensive war strategy in order to enhance Russia's geopolitical gains. It is not secret that Crimea is a strategic territory to Russia. Crimea host Russia's navy fleet which gives her strategic advantages on the sea front. A conclusion can be made that cyber-warfare can be sometimes used to influence security strategies among states.

Georgia

These were a series of well-coordinated attacks on strategic information centers in Georgia that that were conducted by Russia. The attacks were done systematically to aid the Russian military in the armed conflict. Accordingly, "the usage of cyber-attacks in an armed conflict originates from the 2008 Russia-Georgia war. A mass cyber-attack undertaken parallel to on-going military operations is the first precedent of the usage of cyberspace in armed conflicts."[1] The antagonistic relationship between the two nations emanating from geopolitical, legal, cultural and economic suspicion has led to a geostrategic conflict between the two nations. Hackers orchestrated well-coordinated attacks on Georgia. Targets included media houses, banks and transportation just few weeks after invasion by Russian troops. These particular examples speak to the likelihood that exists to attack governments but also the natural integration of cyber-attacks with future kinetic attacks. At the time, many disfigurement and denial of service due to cyber operations were effected against entities in Georgia. The following were some of the targets, Parliament; Presidential websites; Defence; Foreign Affairs, Education ministry; foreign and domestic media sites; banks; and private Internet servers and blogs.

Kyrgyzstan

[1] The Cyber Dimension of the 2008 Russia-Georgia War 5 September 2019 https://www.gfsis.org/blog/view/970.

Internet Service Providers (ISPs) in Kyrgyzstan came under a large-scale DDoS attack, in mid-January 2009 shutting down emails and websites within the country. This nearly took the whole nation offline. These attacks took place when Kyrgyzstan's president had serious pressure from both Russia and domestic actors to close an air base by the USA in the country. These attacks, as reported by The Wall Street Journal, were perpetrated by a Russian cyber-militia.

United States of America

The USA is vulnerable to cyber-weapons the most because its heavy reliance on technology more than any other country in the world. Due to this proneness to attack, the USA is no exception as being a Russian cyber-attack victim is concerned. Previous Russian attacks on the USA have been recorded. However, the researcher will narrow down on the attacks in recent history. The USA suffered a cyber-attack during its 2016 presidential elections. The effects of the attack appeared to favour the now President, Donald Trump. The attacks were sophisticated in such a manner that it discredited another presidential candidate, Hillary Clinton. She was a target because of her criticism of the Putin administration on a lot of global issues. The ability to alter political outcomes in an adversary state has a long way in its survival as she can easily have friendly regimes in competing states.

Cyber-attacks by other Actors

Olympic Games (a.k.a Stuxnet)

This cyber-attack is believed to have been a joint operation between the USA and the Israelis. The primary objective of this operation was to hinder the Iranian uranium enrichment program. Sanger (2012) narrates that “the Operation Olympic Games was devised as a means to throw sand

in the works of Iran's controversial nuclear program. It was initially embarked upon in 2006 without much enthusiasm, as a preferable alternative to withdrawing objections against an Israeli air strike against Iran's nuclear facilities." From this it is abundantly clear that states can use cyber warfare to enhance their foreign policy.

It is also an open secret that the USA has vested interests in the Middle East region and the well documented hostile relationship with Iran has a potential of hindering those interests. The USA had gathered information of Iran developing nuclear weapons in direct violation of the Nuclear Non-Proliferation Treaty (NPT) of 1968. This operation was a success because it managed to infect industrial control systems and sabotage high-speed centrifuges while getting the Iranians to blame themselves or their suppliers for the problems. According to the Christian Science Monitor, "Stuxnet had been inside Iranian networks for over a year, but the nuclear scientists initially thought their facility was just suffering from a series of random breakdowns. The scientists just kept replacing the broken centrifuges with new ones, which would then get infected and break again."[2]

Singer and Freidman (2014) reveal that, "states are now entering an arms race where countries start stocking weapons; only it is not planes and nuclear reactors they are stocking, but its cyber weapons. Within this context, some cybersecurity and public policy experts have declared that cyber warfare is imminent and the U.S.A and other nations must respond – a call to action reminiscent of the cold war era."

2.6 Perceptions on Cyber Warfare

[2] Mark Clayton, How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant, CHRISTIAN SCI. MONITOR (Nov. 16, 2010), http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyberweapon-targeted-Iran-nuclear-plant.

In order to address the questions posed by this research there in need to understand the concept of cyber warfare from the different perspectives of all the political actors involved in the cyber arena. Many global players have since appreciated the need to invest in robust and reliable ICT infrastructure. What remains to be seen are the reasons of bolstering one's infrastructure. For those in business a vibrant ICT infrastructure may bring a competitive advantage thereby improving the profitability of the entity. But can the same be said for states that exist in a world were self-preservation is the main objective? It will be naïve to see no need for states to invest in technology. For states to be able to deliver on their mandates a good ICT infrastructure is a conduit. Again the digitization of states makes them prone to aggressors on this platform although not physically.

As earlier on alluded to, the USA's view of ICT infrastructure as national strategic assets whose protection is a worthy national security policy will ensure that the infrastructure is secure, trustworthy, and resilient. The USA will deter, prevent, detect, and defend against any attacks and recover quickly from any disruptions or damage to the infrastructure. These views portray a very gloomy picture of the cyber space. To the USA the cyber space must be a place where people do as they wish, that is, a jungle without rules or values to talk about and the only way to survive is to make one strong and a live to the activities taking place there. Treating the ICT infrastructure as a 'strategic national asset' testifies the importance of this infrastructure to the well-being of the USA as a state. One will assume that due to the threats that exist in the cyber space, the USA believes that protecting the infrastructure should be a national security objective.

If the words of current French President are to be assumed as the national policy on cyber warfare then the French perception on cyber warfare adds another dimension worth discussing. On the 24th of May 2018 during a joint news conference with President Putin in St. Petersburg, President Macron said, "this is what I can say about cyberattacks or war of words in the press and other

issues. Action always causes reaction. If one does not want to get a reaction he does not like, rules for actions need to be set. When the humanity invented nuclear weapons, everyone realized how dangerous it is and agreed on rules, which were aimed at preventing a tragedy. It is obvious that cyber now is a most important field affecting millions of people. Let us agree on how we work in it."[3] Here it seems the French are advocating for rules of engagement to be agreed upon so that some element of cyber warfare being an asymmetrical warfare be eliminated.

According to Rowe (2019), cyber warfare still sounds like something out of a near-future 80s movie to many, but we're currently locked in a Cold War-style cyber showdown, and a full-blown cyber war isn't out of the question. These fears are also highlighted in the speech given by the Russian Presidential Spokesman Dmitry Peskov who said that a cyberwar between the US and Russia was a "hypothetical possibility." He also stated that "it was President Putin who has on numerous occasions sought to initiate international cooperation to counter any sort of cyber-crime," and that "our American partners never responded to our initiatives."[4]

2.7 Conclusion

In this chapter, the researcher discussed the research topic in the context of available literature, focusing particularly on the secondary objectives. The Russian foreign policy was examined particularly from the Soviet Union era. The concept of cybersecurity was explored in relation to national security. The researcher also put forward various incidents of cyber-attacks perpetrated

[3] Putin on cyberwarfare: Action causes reaction, you don't like reaction – let's talk rules — RT World News Russian President Vladimir Putin (R) and his French counterpart Emmanuel Macron attend a news conference after the talks in St. Petersburg, Russia May 24, 2018. Grigory Dukor © Reuters https://www.rt.com/news/427709-putin-cybersecurity-rules-reaction/

[4] US cyberwar against Russia is hypothetical possibility, says Kremlin spokesman - World - TASS https://tass.com/world/1064123 MOSCOW, June 17 2019. /TASS/

by different actors in the international system. A historical background of the Russian foreign policy was also given. In this chapter, the researcher also traced the origins of the Russian cybersecurity policy. The next chapter is the research methodology.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter is based on philosophies and assumptions which will illustrate how a research was conducted. The chapter discusses how data was collected from different sources. It further outlines the research design, data collection methods as well as tools used, sampling criteria and lastly ethical issues considered throughout the research process. The objective of this chapter is to give justification to the methods chosen by the researcher to reach the stated research objectives in Chapter One.

3.1 Research Design

The researcher uses two different perspectives to research. Maree and Pieterson (2007) state that, "research is about understanding the world, and your understanding is informed by how you view the world, what you view understanding to be and what you see as the purpose of understanding". According to Pandey and Pandey (2015) the term research, "comprises of two words're' and 'search' meaning to search again." Research here is viewed as a method of acquiring new learning material to the knowledge body. The two scholars agree that research design is the roadmap in the journey to collection, measurement and analysis of data. Kothari (2004) views that, "among the different reasons for a research design is to facilitate the smooth sailing of research operations, for example, ascertaining the required resources, time, effort and money." Adams and Schvaneveldt (1991) state that, "research designs are plans that guide decisions as to when and how often to collect the data to gather, from whom and how to analyse the data. They go on to say that the specific meaning of research design refers to the types of study which include cross-sectional studies, time-series analysis, case studies and experimental designs." Kerlinger (1986)

describes it as, “a plan and structure of investigation so conceived to obtain answers to research questions. The research design therefore refers to the planning of the approaches to solve a research problem.”

In this instance a research should answer the research questions and can be used as the test instrument for the hypothesis of the study. It should link the abstract, perceptions and research questions with the pragmatic world’s complexities and challenges. This therefore entails that a research design should be specific, expansive and flexible enough to address the complexities whilst guiding the researcher towards relevant data. The research design chosen in this research influenced the selection of the research methods used.

This study adopted a case study approach. According to Yin (1994) a case study is, “preferred when the ‘how’ or ‘why’ questions are being posed. When the investigator has little control over events, and when the focus is on contemporary phenomena within some real life context.” Gilbert (2008) cited by Koul (2000), argue that, “a case is an approach whereby a particular instance or a few carefully selected cases are studied intensively.” Koul (2000) contends that, “in a case study, the case being studied can be easily generalized for similar cases or at least provide insights.” The case study choice is informed by the desire to understand how cybersecurity is informing national security policy from the Russian perspective and how actors are responding to cyber-attacks. The relevance of cyber warfare to Russian security policy is also under investigation in this study. Researching on national security issues poses some challenges due to the secretive nature of the subject.

In the quest to achieve the research objectives an interpretive case study was used to investigate the Russian foreign and security policies in the auspices of cyber warfare. Although other actors are investigated the primary target was the Russian policy. Hence the method was carefully chosen as an extension of the researcher’s substantive questions and epistemological orientation.

A qualitative research method was chosen due to its suitability for this research. McLeod (2001) argues that, "through qualitative research one can explore a wide array of dimensions of the social world, including the texture and weave of everyday life, understandings, experiences and imaginations of our research participants, and ways that social processes, institutions, discourses or relationships work, and the significance of the meanings that they generate." McLeod (2001) states that, "the primary goal of qualitative research is to develop an understanding of how the world is constructed." He further points out that, "the world can be viewed from different perspectives. Thus qualitative research aims at knowing how particular individuals or groups understand the world." McLeod (2001) further argues that, "people already have an understanding of the world based on their norms and values. Such knowledge is however, far from being coherent and consistent. Qualitative research aims at providing formal statements and conceptual frameworks that provide new ways of understanding the world. The qualitative research method then seems appropriate for the purposes of this study, aiming at developing a consistent and coherent knowledge of how cyber warfare is informing national security policy."

This approach is weak due to its subjectivity, no standard way of data collection and analysis. The process is also time consuming and expensive.

3.2 Research Methodology

The research was informed by the qualitative research methodology which gives respondents an opportunity to completely air out their answers to questions asked. Qualitative research is associated with interpretivist approach and ideographic tools (Henning, 2004). Babbie and Mouton (2001) describe qualitative research as, "referring to meanings, definitions, concepts, characteristics, metaphors, symbols and description of things." Similarly, Creswell (2012)

defines qualitative research as, “philosophy that is intended to deeply explore, understand and interpret social phenomena within a natural setting.” Qualitative research is interactive as it is conducted in the field.

The study population comprised of officials responsible for cybersecurity in the Ministry of Foreign Affairs, Ministry of Defence, Interpol Cyber Centre (Harare), academics, and renowned experts in the field of international relations. It is because of the various groups in the population that guided the researcher to base and conduct the study under the guise of qualitative research.

Creswell and Clark (2011) are of the view that qualitative research data collection methods include examining documents, observing behaviour and interviewing participants. Corporate websites, annual reports, group discussions and interviews were also carried out in order to get in depth information regarding how cybersecurity is viewed and implemented by various actors in the international system. The researcher adopted the multi usage of sources of data as compared to a single method of data collection to avoid bias. Qualitative research mainly focuses on interpretation of what is seen, heard and understood by the researcher (Creswell and Clark, 2011).

3.3 Population

According to Pandey and Pandey (2015), population is, “the entire mass of observations, which is the parent group from which a sample is to be formed.” According to Cohen, Manion and Morrison (2000), “a population is a collection of all elements that are being studied and about which we are trying to draw conclusions.” In other words a population has some common characteristics to the researcher. The study population comprised of officials responsible for cybersecurity in the Ministry of Foreign Affairs, Ministry of Defence, Interpol Cyber Centre

(Harare), academics, and renowned experts in the field of international relations. These were chosen due to their direct linkage to national security.

Academics from the Department of Political Science at the University of Zimbabwe, Centre for Defence Studies, Zimbabwe Defence University, Zimbabwe Institute of Diplomacy and Midlands State University were also interviewed. This is because their expert views about cybersecurity were critical to this study. As Strategic Studies and International Relations experts their participation was of value to this study.

3.4 Sampling

According to Jackson (2011), a sample "is a small proportion of a population selected for observation and analysis." Jackson (2011) further argues that, "sampling is done haphazardly; rather, it is done in a systematic random way." The study employed both probability and non-probability sampling techniques. Purposive and stratified samplings were used.

Purposive sampling was employed to select government institutions with links to state security. A purposive sample was used to select government officials, academics, and personnel in the cybersecurity field due to their expertise in cybersecurity. Graziano and Raulin (2000) define purposive sampling as, "selecting participants for their ability to provide rich information. It allows the researcher to carefully select cases that can typify or shed light on the subject of study." This technique was chosen as a way of identifying participants with expertise in addressing research objectives.

Purposive sampling besides being the best approach in qualitative studies, it is subjective as the researcher forms a view in choosing respondents. The findings cannot be replicated to another population.

3.4.1 Sample size and its determination

The sample size refers to the number of objects selected for the study. Singh and Masuku (2014) define sample size determination as, "the technique of electing the number of observations to include in a sample." According to Hussey and Hussey (1997) sample size is, "a subject of population and should represent the main interest of the study." To Brink (1996), a sample is "a part or fraction of a whole or subset of a larger set, selected by the researcher to participate in a research project". Singh and Masuku (2014) argue that, "this is the total number of individuals (or groups) randomly assigned to the intervention and control groups.This generally depends on the cost of data collection and statistical power base and variance."

Stratified sampling was employed to choose participants representing different organisations and groupings. Participants were further grouped by gender. The researcher had prepared the black and white cards which he asked them to select. Those who selected black cards were automatically chosen. A total number of 15 respondents were selected for this study, while a total number of 10 key respondents from the various institutions were included in the study. The entire sample was made up of 35 respondents.

Babbie (2004) acknowledges that, "a purposive sample is selected on the basis of knowledge of a population, its elements, and the purpose of the study." These groups of key respondents were specifically chosen due to their information rich characteristics. Steinke (2004) says, "Purposive sampling also known as judgmental sampling is a non-probability technique that involves

choosing a sample from a limited number of people that have expertise in the area being researched."

3.5 Data Collection

Data collection is an important part of qualitative research. The research was guided by in depth interviews, focus group discussions and document analysis as data collection techniques. This was done to circumvent potential validity problems. Case studies, however, fail to advance sufficient operational measures to collect data grounded on subjective arguments. Subjectivity of information from informants tends to be contradictory and diverse thereby reflecting differences in the nature of responses and individual knowledge given how one is asked to provide information.

Multiple sources of evidence, however, must be used to provide reliable information. Jackson (2011) argues that, "strict and rigid adherence to a single method when doing fieldwork become like confinement in a cage. Therefore, by implementing different methods of data collection the researcher intended to increase the authenticity of facts gathered, since the different methods complement each other." Several sources of information render the findings and conclusions more accurate and convincing.

3.5.1 In-Depth Key Informants Interviews

The study used data generated through semi-structured interviews that were conducted between July and September 2019. Interviews were used as an attempt to understand the concept of cyber warfare. According to Brink (1996), "an interview is a method of data collection in which an interviewer obtains responses from the subjects in a face to face encounter or through a telephone

call or electronic means." Through the designing of the semi-structured interview instrument the researcher understood many contradictory and different layers of meaning. Graziano and Raulin (2000) argue that, "semi-structured interviews may yield much more than those that are fully structured if conducted well." Due to the nature of the research which sought to investigate and understand how the concept of cyber warfare is influencing national security policies, semi-structured interviews appeared to be the best option for comprehending the opinions, expressions and attitudes of different individuals' experiences.

An interactive–relational approach to interviews was used. McBurney (1994) points out that, " the effectiveness of the interactive–relational approach in interviewing as compared with the purely fact finding approach which he regards as lifeless rather than effective because it ignores the dynamics between the interview and the interviewee." His opinion is that, "by developing an interactive and relational stance, it is possible to access information that would not emerge through formal and structured questioning alone." This approach is most suitable especially when conducting interviews looking at national security issues since it establishes a relationship with respondents and this led to the giving out of more information. Interviews facilitates data gathering through dialogue or even arguments with an opportunity to make follow up questions for verification.

The down side of this approach is that it consumes time since the degree of understanding questions vary and also taking notes of the interview may require repeating time and again. Also, participants may fail to reconstruct their memory, limited skills to express one's views and lack of insight. Short and clear questions were crafted to overcome this.

Individual interviews were recording using a cell phone with clear consent from the interviewees. Nineteen members were interviewed with their informed consent, of the nineteen twelve were

males and seven were females. These individuals were key informants and their opinions were important to this research. Interviews were meant to give further explanations as well as throwing some light on important issues tabled by prior respondents. It was also done to follow up and explore questions suggested by gaps or contradictions in the previous interviews carried out on various institutions, organisations and groups. Interviews provided richer insights and answers that are valued valuable to the study which might have been missed by other methods. Apart from seven, all interviews were conducted in Shona even though those interviewed understood English the researcher wanted them to freely express their sentiments. This made the interviews more cordial as the researcher was able to rephrase and repeat with proper emphasis as well as explain more on some questions.

The respondents were assured of the confidentiality issues whilst every interview was recorded for decoding purposes. The researcher further adopted the probing method to ensure that essential information regarding the study was acquired. Mainly open ended questions were used to give respondents room to give details on issues discussed.

3.5.2 Document Analysis

Carrying out document analysis is essential in social science research. This involves scrutinizing written documents containing essential information regarding the subject understudy. The process thus requires intensive reading and analysing discourse relating to field research. Eisenhart (1989) describes document analysis as, "referring to various procedures involved in analysing and interpreting data generated from examination of documents and records relevant to a particular study." With respect to document analysis the researcher relied much on two documents, the Military Doctrine of the Russian Federation of 2000 and 2015. Document analysis helped the researcher in identifying gaps between policy and implementation procedures as well

as to see if there were any loopholes with regards to the law on the conducting of cyber-attacks. The evidence corroborated, augmented and complemented other information sources.

Document review was considered an important data collection method to use in this research for its strength of providing current primary data on issues under study. Internet was also relied on as it gives access to contemporary published journals and articles.

3.5.3 Focus Group Discussions

These are group interviews were a moderator facilitates discussions of various topics. In this study one session was conducted though the researcher had planned to have many sessions. This was due to the unavailability of some members of sample population. The group comprised of five members three from Interpol and two from the academic fraternity. Focus group discussion was carried out because it was inexpensive, quick, flexible and excellent approach to data gathering.

3.6 Validity and Reliability

Winter (2000) states that, "reliability and validity are tools of an essentially positivist epistemology."

3.6.1 Validity

Leedy (2000) states that, "validity is the extent to which an empirical measure clearly reflects the intended meaning of an issue being discussed, for example, how accurate certain questions in the endeavour to answer given research questions are." According to Winter (2000), "the traditional criteria for validity find their roots in a positivist tradition, and to an extent, positivism has been defined by a systematic theory of validity. Within the positivist terminology, validity resided amongst, and was the result and culmination of other empirical conceptions: universal laws,

evidence, objectivity, truth, actuality, deduction, reason, fact and mathematical data to name just a few". The research method inherently has a bearing to the assessment of the validity of a study. In this study the researcher purposively used the qualitative key informant's in-depth interviews and document analysis to gain invaluable information. Validity in qualitative research seeks to qualify checks and balances in the field of research.

3.6.2 Reliability

Joppe (2000) defines reliability as, "the extent to which results are consistent over time and an accurate representation of the total population under study is referred to as reliability and if the results of a study can be reproduced under a similar methodology, then the research instrument is considered to be reliable." The test and retest method can also be applied to measure reliability and the results should still replicate.

To Joppe (2000), "if we are dealing with a stable measure, then the results should be similar. A high degree of stability indicates a high degree of reliability, which means the results are repeatable." Joppe (2000) states that, "the test-retest method can be problematic as it can make the instrument, to a certain degree, unreliable." To her, "the test-retest method may sensitize the respondent to the subject matter, and hence influence the responses given. We cannot be sure that there was no change in extraneous influences such as an attitude change that has occurred." There are various methods that can be used to ensure enhance validity and reliability of the research. The researcher administered questionnaires through a pilot study where the researcher focused on grammatical and technical aspects of questionnaires such as spellings, double barrelled questions being removed and rephrasing some of the questions. Member checking is another method that the researcher used. According to Creswell (2012), despite the period in which the researcher conducts member checking this phenomenon is essential for authentication of data collected. Patton (2002) encourages the use of triangulation by arguing that, "triangulation strengthens a

study by combining methods. This can mean using several kinds of methods or data, including using both quantitative and qualitative approaches."

However, this idea of combining methods is challenged by scholars such as Barbour (1998) who argue that, "while mixing paradigms can be possible but mixing methods within one paradigm, such as qualitative research, is problematic since each method within the qualitative paradigm has its own assumption in terms of theoretical frameworks we bring to bear on our research." The researcher made use of triangulation in order to ensure reliability and validity without withstanding the importance of the paradigm in qualitative research which according to Crotty (1998), "is constructivism which views knowledge as socially constructed and may change depending on the circumstances." Crotty (1998) defines constructivism from the social perspectives as "the view that all knowledge, and therefore all meaningful reality as such, is contingent upon human practices, being constructed in and out of interaction between human beings and their world, and developed and transmitted within an essentially social context."

3.7 Data Presentation, Analysis and Interpretation Procedures

Polit and Hungler (1993) argue that data in research should be analysed in order to give it meaning through classifying and analyzing. Data presentation, analysis and interpretation in qualitative research involve deducing non-numeric information gathered by the researcher.

The approach is, however, relevant where the researcher is aware of the probable responses from the participants. This approach is prone to bias and predetermined interpretation as such inductive approach will be used to compensate such weakness. The researcher used a pragmatic thematic content analysis approach achieved through identifying the relevant themes and categorizing them into sub themes for interpretation purposes.

In qualitative research, interpretation of data begins soon after the commencement of data collection. According to Stake (1995), "qualitative data analysis is an iterative and reflexive process that begins as data is being collected rather than after data has ceased." The researcher therefore adopted Stake's approach were data was analysed as the study progresses. This approach enabled the researcher to continuously re-examine the research questions upon emergence of new information. The researcher would continuously adjust the interview guides to fill in the gaps discovered as the research progresses. In this regard, further clarity was sought upon discovery of fresh evidence pertaining to the study.

3.8 Ethical Considerations

Zvekic (2000) "bemoans the rampant weakness among researchers of failing to respect the preponderate conflict between the researcher and the researched." In this spirit, the researcher will always alert himself to the rights of the researched. Among such rights are the rights to withdraw at any time, freedom from physical and psychological harm and the general requirement that the researcher should be as professional, secret and honest as possible.

According to Saunders et al. (2012), "research ethics provides guidelines for the responsible conduct of research. In addition, it educates and monitors scientists conducting research to ensure a high ethical standard." Saunders et al. (2012) define ethics as "the appropriateness of behaviours in relation to the rights of those who become the subject of your work or are affected by it." Whilst Babbie and Mouton (2001) emphasize that social research often represents an intrusion into people's lives therefore research ethics should be consistently observed. The major rationale for ethical considerations when carrying out a research is to protect the respondents or participants. Violations of research ethics adversely affects the research outcome and negatively impacts on

any future studies. The researcher will be cognizant of the informed consent, anonymity and confidentiality as some of the ethical guidelines.

3.8.1 Voluntary Informed Consent

According to the Nuremberg Code (1947), "valid consent in research should be properly informed and freely given without pressure such as coercion, threats or persuasion." The researcher was guided by this fundamental code of conduct. The respondents were made aware of their rights, purpose of the study, the study procedures to be followed and what the researcher intends to do with the research afterwards. The researcher made use of documents acquired from the Department of Peace and Governance that declares the researcher as a bona-fide student of the faculty.

3.8.2 Anonymity and Confidentiality

This principle generally refers to the concealment of the respondents' identity in a research. The British Sociological Association Code of Ethical Practice (BSA:704) states that, "research participants should understand how far they will be afforded anonymity and confidentiality and should be able to reject the use of data gathering devices such as tape recorders and video cameras." Inmates and other respondents require assurance that their names will not be mentioned anywhere in the research. The researcher used pseudonyms to ensure protection of respondents. Only key informants were identified, but consent had to be sought from them before mentioning their names. The researcher used codes on completed questionnaires and observed security procedures in storing data to ensure limited access to information collected.

3.9 Chapter Summary

The chapter presents the research philosophies used to guide the research. The research methodologies used to carry out and validate the research were also deliberated on, and these included research design, sample design, sampling procedures, data collection and data interpretation and analysis. The chapter further presented the research as case studies of the ethical considerations were also discussed in the chapter as they are a pivotal component of any study.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

4.0 Introduction

This chapter presents and analyzes the research findings. According to de Vos (2002), "data analysis is the process of bringing order, structure and meaning to the mass of collected data." The findings are discussed, presented and interpreted in this section of the study. The research results give answers to questions in Chapter One above. Data was collected through three different data collection techniques namely interviews, focus group discussions and document review. The respondents were composed of officials responsible for cyber security from the Ministry of Defence, Ministry of Foreign Affairs, Interpol Cyber Centre (Harare), and academics from different institutions of higher learning as well as renowned experts in the field of international relations based in Zimbabwe.

4.1 Demographic information of participants

Data related to those interviewed was gathered from officials responsible for cyber security from the Ministry of Defence, Ministry of Foreign Affairs, Interpol Cyber Centre (Harare), and academics from different institutions of higher learning as well as renowned experts in the field of international relations in Zimbabwe. Interviews were carried out whereby key informants from these fields were purposively sampled. Table 1 below illustrates interview responses of the target population.

Table 1: Interview targeted population and the responses.

Target group	**Target responses**	**Actual responses**	**Response %**
Members from the Ministry of Defence	5	3	60%
Members from the Ministry of Foreign Affairs	5	4	80%
International relations Analysts	4	2	50%
Academics	4	3	75%
Interpol Cyber Centre	3	3	100%
Other Security Services	4	3	75%

Table 1 above denotes demographic information of the study. These statistics are also presented in Figure 1 below. The researcher, due to time and financial constrains had intended to conduct 25 scheduled interviews. However, eighteen interviews were conducted; representing a 72 percent response rate which the researcher felt was adequate for analysis.

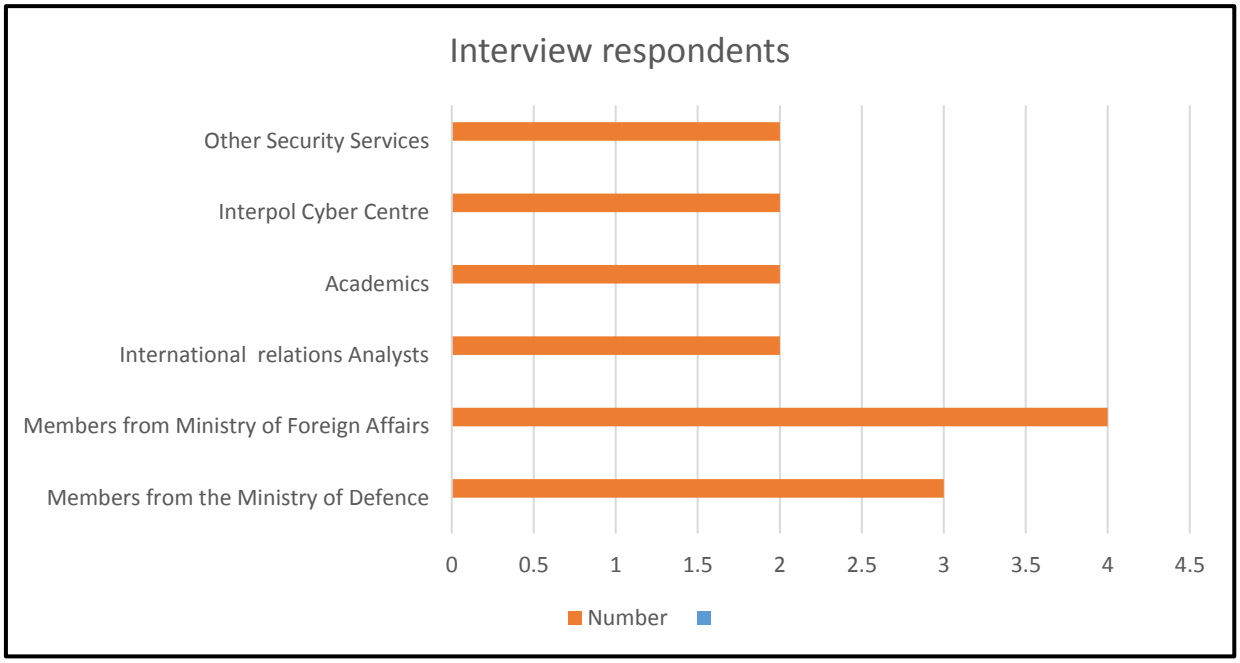


Figure 1. Interview Respondents

4.2 Presentation of Research Findings

4.2.1 What is the Russian Foreign Policy from the perspective of national security?

The Russian foreign policy is hinged on the belief that its threats are existential. Previous administrations in Moscow including the current President Putin's administration are convinced that their existence is a big inconvenience to their adversaries especially the Western block. This belief coupled with her desire to be a global super power has led Russia to adopt an aggressive foreign policy when it comes to her security. This view was echoed by Analyst A who argued that;

> *In recent years the Russian foreign policy has been assertive. For the past two or so decades, Moscow has demonstrated her unwillingness to compromise on any threats against her no matter the size of the threat. For example, the annexation of Crimea in 2014 testifies to the aggressiveness of the Russian foreign policy. He further argued that this may be attributed to her quest to counter efforts by NATO to continuously reduce former Cold War borders eastwardly and getting closer to Russia.*

With her aggressive foreign policy under President Putin, Russia annexed Crimea in contrast to the 1994 Budapest Memorandum which assured Ukraine protection against threats and use of force within its territory. Russian foreign policy interests in Ukraine centres on various factors which according to Nygren (2008), are both geopolitical and economic.

Analyst B, however, viewed the Russian foreign policy as one which is there to safeguard her existence hence she termed it a defensive foreign policy. She viewed the Russia-Ukraine crisis as emanating from Russia's desire to protect herself from external threats. She further highlighted that;

> *Russian strategists wanted to keep Ukraine as a buffer state. Russia disliked the idea that Ukraine would become a member of NATO or EU. Ukraine belonged to the Russian sphere of influence in the eyes of Moscow and has been preventing Ukraine's wish to be a member of NATO for a long time.*

The analyst`s arguments are in line with what is found in Chapter 2. Ukraine's ambitions to join NATO are perceived by Russia as a serious threat that needs to be stopped by whatever means possible. According to Radlin and Reach (2017), "Russia feels insecure since it lacks major natural boundaries which act as buffers." It is now clear why Russia`s foreign policy is deeply swayed by insights of danger and susceptibility. This situation has also not been made easy by its past foreign invasions and this has resulted in a national discourse of susceptibility and concern about foreign danger. Consequently, her grave security concerns have led her to prioritise a regional foreign policy. Consolidating relations with surrounding nations possibly exert her direct control over her neighbours thereby enabling her to create buffers for foreign invasion.

Officials from both the Ministry of Defence and the Ministry of Foreign affairs were of the view that;

> *..... it will be naïve to be content with what meets the eye when analysing the Russian foreign policy. President Putin's external policy has its umbilical code attached to the Soviet Union philosophy of national sovereignty and anti-colonial resistance. Therefore, the Russian foreign policy in the perspective of national security can be understood if traced back to the Soviet Union.*

The above view echoes Light (2015)'s argument that, "Russia's main foreign policy interest and goals have remained consistent since the post-Soviet Union era." It can be further argued that, the collapse of the Soviet Union in 1991 did not go with the military acumen of the Russian military experts. It therefore becomes undeniable that modern day Russia inherited a rich tapestry of military thought from the Soviet Union. The current political and military thinking that drives

the new Russian discourse is grounded in the Soviet historical experiences and also linked to the ideological prisms of the Communist Party of the Soviet Union. This view is also shared by scholars such as Lukyanov (2016), Kuchins and Zevelev (2012), Kotkin (2016) and Laquer (2015) who also argue that, Russia`s foreign policy is mainly driven historically by its struggle to be recognised as a super power.

It can be noted that the preceding arguments bring about two important dimensions of Russian foreign policy. Firstly, there is evidence that the current foreign policy borrows a lot from the former Soviet Union perceptions of world dominance. One can argue that it is still Moscow's desire to be a global political power. Secondly, the foreign policy of Russia is underpinned on her protection from constant threats from the West. These views are in line with the argument raised by Lukyanov (2016) in Chapter 2 that Russia has historically considered Central Asia as its zone of influence, a chessboard where she will play to dominate.

Analyst B brought to the fore another dimension in respect to national security as perceived through Russian strategic thinking. She argued that;

> *Russia is maintaining its position through its superior use of information as a tool of asymmetric statecraft. All Russian leaders consider information operations as a decisive tool of state power. They deliberately engage in constant international competition in the information domain. These coordinated efforts to project influence using information and disinformation makes Russia`s foreign policy unique. Whereas other states' information operations are generally guided by facts, Russia's foreign policymakers create 'facts' to be broadcasted to targeted audiences in order to achieve strategic objectives.*

4.2.2 What are the origins of Russia's cyber policy?

The above view echoes current Russian thinking as highlighted by scholars such as Thomas (1998) and Softa (2008). Accordingly to Softa (2008) Russia's focus is also now on issues to do with information resources. Similarly, Wirtz (2015) also points out that recently, "Russia has found her reliance on using cyber capabilities as a tactic to achieve her strategic goals both in her near-abroad and against Western countries." These perceptions about Russia's strategic thinking makes one argue that cyber capabilities have taken centre stage in global political wars this also means that cybersecurity has become a cause for concern for national survival which is an area l now turn to. The Russian view to cybersecurity is one of its own. The view is completely different from Western cybersecurity thinking. This can be evidenced by the way Russia defines cyber warfare and how the Kremlin employs its cyber capabilities. As such in Chapter two, arguments were that the Russian cyber policy is grounded on her history and past grievances as well as the constant insight that Russia is constantly under siege. Russian military theorists strongly believe that the lack of control over information resulted in the collapse of the Soviet Union. This then led the current Russian state to work on strategically improving its cybersecurity technologies. As such, an academic indicated that;

> *The most significant instance of a Russian cyber-attack happened in Estonia in 2007. At the time, tensions were high between Russia and the former Soviet State, and the Kremlin authorized a campaign which targeted Estonian governmental agencies and businesses through the use of massive distributed denial of service attacks that shut down countless websites that were essential to the functioning….*

One can argue that although a notable cyber–attack came in 2007 it does not mean that Russia had been inactive on issues to do with cyberspace. Allen and Moore (2018), point out that "modern Russian information operations are shaped by many traditions. Russian leaders have

long placed exceptional value on using information to manipulate their enemies." Scholars such Iasiello (2017), Smith (2014) and McGuinness (2017) note that the attack on Estonia was not the last one. According to White (2018), "Russia also demonstrated her cyber capabilities during the Russo-Georgian war." In this regard, an academic also stressed that;

> *Sometime in 2008, Russia coordinated a hybrid of attacks during the Russo-Georgian War. Cyber-attacks were conducted from Russia against Georgian government and media websites, while at the same time Russian troops were crossing the Georgian border. The Russian cyber-attacks affected practically all Georgian government websites, crippling the state's ability to respond to the conflict. The objective was to make it difficult for information to spread out to the rest of the world.*

The above responses echoes the arguments raised in Chapter two by scholars such as Iasiello (2017) and Smith (2014). White (2014) is of the view that cyber-attacks had become an established tool of statecraft. Likewise, Iasiello (2017) also points out that, "cyber-attacks in the Russia-Georgia war reaffirm the Russian view of cyberspace as a tool for psychological manipulation and information warfare." As such one can argue that Russia has never sat on her laurels as far as the cyber domain is concerned. This is because she is aware that such threats will remain constant. The argument is that ever since the attack on Estonia, the Russian digital signatures has been reported to be found on a number of networks. An analyst also highlighted that;

> *…The officials in Moscow, are in an unending and winding struggle to control information. The struggle is both domestic and foreign. The advent of the internet and the associated technologies leading to the free flow of information has presented challenges as well as opportunities.*

The above view compliments opinions proffered by researchers such as White (2018). The argument is that, "while the USA military has established an understanding of cyberspace as a discrete domain of warfare that deserves its own doctrine, its own troops and its own unique menu of lethal and non-lethal effects, Russia treats cyberspace as a subordinate component to its holistic doctrine of information warfare." As such one might argue that Russia is seeking to achieve when it carries cyber-attacks on other states. However, realist scholars have always argued that actors in the international system are seized with the ultimate objective of self-survival hence they are pre occupied by safeguarding their self being in a world driven by the 'Self Help" principle. The existence of Russia has been and will always be a threat to the Western block hence, the reason Russia has taken an aggressive as well as defensive approaches regarding cybersecurity and cyber warfare.

This might be on reason why Russia has continued such an aggressive cyber strategy on other states. It can be further noted that Russian activities on the cyber space are complementing or it fostering the underpinnings of her foreign policy. An official with the Ministry of Defence summarised the Russian objectives in the cyber domain as follows;

> *First and foremost Russia sees the need for territorial compensation hence the cyber-attacks are used for capturing territory without resorting to conventional military force. Creating a justification for conventional military action is also an objective for the Russian military strategists. The last objective, is that the Kremlin seeks to use cyber operations in lieu of military action or war to create tension and distress in Western governments.*

The above view compliments opinions proffered by researchers such as Segal (2016) and Thomas (2015) in Chapter two. They highlighted that, "Russia seeks to achieve political objectives without the utilisation of military force and in combination with conventional means as a tool to create a favourable response from the world community." According

to Appel (2008) this means that, "the conduct of Russia in the arena of foreign affairs suggests that Russia is continuing to vacillate between its aspiration to keep the United States 'global ambitions in check and the state of reality that requires it to bandwagon with the United States". One can also concur with the Ministry of Defence official by pointing out that in 2014, Russia embarked on cyber-attacks on Ukraine which affected its power grid a move which successfully ended up with the annexation of Crimea. Russia`s meddling in political processes in Western capitals also speaks to these objectives. In Chapter two, it was observed the USA suffered a cyber-attack during its 2016 presidential elections as an attempt by Russia to favor President Donald Trump over his opponent whose view against Russia was extreme.

4.2.3 How have states responded to Russia's cyber-attacks?

In Chapter two, arguments raised were that, the continuous use of cyber tactics by Russia and her ongoing development of more lethal cyber arsenal is now of grave concern to many global players. The USA seems the most worried in this game. Russia has been threatening the USA with realistic threats both domestically and internationally. An analyst stressed that;

> *On the global front Russia seems to be keen to increase its sphere of influence by territorial expansion. This is not in any way good for the USA. A wider influence of Russian thought and expansion of pro-Russian policies is a setback in areas where the USA has worked to promote democracy and peace. To the USA this may mean the rebirth of the Russian desire to reassemble the Soviet Union as seen in Estonia, Georgia, and Crimea cyber-attacks which can play a key role in these territorial gains.*

Similarly, analyst A further explained that the Russian threat to the USA was also internal. The most frightening reality is the ability of Moscow to meddle in Washington's internal political systems. He highlighted that;

> *Domestically, Russian cyber-attacks can destabilize the USA government by creating rifts and tensions amongst the American populace through the spread of false information and fake news. As seen by the hacks during the 2016 Presidential Election. This means Russia's use of cyber-attacks can undermine American democracy by allowing for a foreign nation to alter the minds of citizens. Attacks by Russia can also cripple the government's ability to function towards the service of its citizens.*

In Chapter two, it was also noted that Russia is becoming interested in influencing political processes in the West. This means that using her cyber capabilities Moscow can now prop up friendly regimes in the West and enhance the chances of weakening West aggression. One can argue that due to the Russian threats the USA has swiftly stepped up its passive cyber space presence into an aggressive one. An official with the Ministry of Defense attached to the department that deals with cyber security has this to say;

> *The United States established the United States Cyber Command, the arm of the Pentagon that runs the military's offensive and defensive operations online. It is interesting to note that the USA feels that the Russian attack was really damaging on the Pentagon therefore they are now deploying cybertools more aggressively…. Recently, attempts have been made by the Americans to infiltrating Russia's electric power grid. Since at least 2012 the United States has put reconnaissance probes into the control systems of the Russian electric grid. This is a clear retaliation against Russian actions on the cyber domain.*

Sanger (2012) also note that, "the United States has a persistent presence in foreign computer networks around the world, because if she is not already buried inside those networks, it will be difficult for her to see an attack coming and this will render her incapable of retaliating." He further argues that one has to go on the offensive to really be on the defensive and this can only be achieved by living in those adversaries' networks. Such thinking is premised on realist perceptions of security in that realists believe that offensiveness is best guarantor of security. And also assume that human nature is generally evil and states are anarchic in nature and they seek to protect their interests at any cost.

4.2.4 Document Analysis

A document analysis was carried out to answer some of the questions. The following two documents were analysed by the researcher, that is, the Military Doctrine of the Russian Federation of 2000 and the revised 2015 version. These two documents are the most critical documents because they provide key guidelines to the Russian military operations. In other words, these documents act as the Russian military bible. The documents' preface highlight that;

> *"….Military Doctrine of the Russian Federation is a system of officially adopted State views on the preparation for armed defence and armed protection of the Russian Federation. The Military Doctrine, based on the analysis of military threats and threats to the interests of the Russian Federation and its allies formulated the basic provisions of the military policy and military economic support for the defence of the state….."*.

The above preface from the Military Doctrine of the Russian Federation highlights the implementation of Waltz (1979)'s view which argue that , "States in the international system serve their own interests by following a strict code of self-help due to absence of any authority above them." Clearly Russia is taking upon itself to protect her national interests against real or

imaginary threats. Again, critically looking at the preface, it was crafted in anticipation of an attack giving credence to Cimbala (2013)'s augments discussed in Chapter 2. Cimbala (2013) attested that there is permanent suspicion in the international system when he said, "Russia's national security concepts and evolving expressions of military doctrine show its fears of surprise attack in the face of NATO conventional military superiority, notwithstanding NATO's declaratory policy of no hostility toward Russia."

From these documents there is a general agreement that points to the fact that there is suspicion in the cyber sphere. The policy documents were crafted as a counter measure to real or imaginary threats from perceived enemies. Major highlights from the documents are presented below.

The analysed documents seem to concur with the sentiments of other participants interviewed in the research on a number of issues. Firstly, the belief that Russia is continuously under threat from external forces particularly the mere existence of NATO and the organisation's unrelenting efforts of getting closer to the Russian boundaries such threat is categorically stated in the documents as a major challenge to Russia's security. Secondly, as alluded earlier on from an interview transcript of one academic participant the documents under review shows that these threats are both internal and external. To support this, the following quote from the Military Doctrine of the Russian Federation was adapted and adopted;

> *"…. actions aimed at violent change of the Russian constitutional order, destabilization of the political and social environment, disorganization of the functioning of governmental bodies, crucial civilian and military facilities and informational infrastructure of Russia…".*

Russia has broadened the spectrum of her military doctrine incorporating issues such as cyber warfare. According to Babadjanov (2008), "the Russian Federation 2000 Military Doctrine was as defensive as other post-Soviet era doctrines but the nature and threat in all areas of national security has changed".

Russians prefer to talk about information warfare rather than cyber warfare. For Russian theorists, cyber warfare is limited to activities on the internet only. Russia has weaponised information and thrives on winning perceptions in every other conflict she is involved in. The following statement from the analysed documents speak to that effect;

> *....the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force" and shape adversaries' behavior in a way that elicits a favorable response..*

Information warfare according to the Russian Federation's military doctrine is akin to what many journalists and civilian analysts have been describing as 'information war'. The Russian concept of information warfare is in fact a synthesis of traditional, old and modern methods (resulting from the current state of universal access to IT technology), military and non-military structures and means of influence. One can conclude that the Russian domestic social order has an influence on her foreign policy.

4.3 Conclusion

In summary, this chapter showed, examined and deliberated on the results of the study. Data presentation was through discussions and analysis. Major findings are that the Russia`s foreign policy is hinged on the belief that its threats are existential. This general feeling of insecurity that confronts Russia is as a result of the lack of major natural boundaries to act as buffers. From this it becomes clear that Russia`s foreign policy is deeply inspired by opinions of danger and

susceptibility. Russia's policy on information is influenced by many historical factors. Russia has put in place incomparable importance on information to manipulate her enemies. Russian activities on the cyber space are complementing or rather fostering the underpinnings of her foreign policy. The United States seems the most worried in this game. Russia has been threatening the USA with realistic threats both domestically and internationally.

CHAPTER FIVE

SUMMARY, CONCLUSIONS, RECOMMENDATIONS

5.0 Introduction

This chapter focuses on the summary, conclusion and recommendations. Recommendations are based on the conclusion of the study. This chapter gives the summary of the whole project. The summary highlights major findings of the study in relation to research objectives and research questions. However, this chapter finally gives some recommendations on the influence of cyber warfare to security policy

5.1 Summary

The broad objective of this study was to determine the influence of cyber warfare to security policy. The research also examines both the theoretical and practical underpinnings of the Russian foreign policy on cyber warfare. In the quest to achieve the objectives of this research there was need to also analyse the Russian foreign policy vis-a vis national security. The research explored and also assessed internal and external factors which are attributed to be at the core of the Russian foreign policy. As such, all forms of threats to Russia were discussed at length. The research further examined the roots of Russian cyber policy also assessing consequences of Russian cyber-attacks. The Russian foreign policy was examined particularly from the Soviet Union era. The concept of cybersecurity was explored in relation to national security. The research also put forward various incidents of cyber-attacks perpetrated by different actors in the international system. A historical background of the Russian foreign policy was also given. The research also traced the origins of the Russian cybersecurity policy.

5.2 Conclusion

The following conclusions have been arrived after a careful and systematic consideration of the research findings in relation to the research objectives and existing literature. Findings show that the Russian foreign policy is shaped influenced and conducted mainly by the belief that its threats are existential. This general feeling of insecurity that confronts Russia is as a result of the lack of major natural boundaries to act as buffers. From this it becomes clear that Russia`s foreign policy is deeply inspired by opinions of danger and susceptibility. Russia's policy on information is influenced by many historical factors. Russia has put in place incomparable importance on information to manipulate her enemies. Russian activities on the cyber space are complementing or rather fostering the underpinnings of her foreign policy. While Russian cyber tactics appear to be evolving, the theoretical and doctrinal underpinnings of Russia's approach to cyber warfare have remained more or less constant. The United States seems the most worried in this game. Russia has been threatening the USA with realistic threats both domestically and internationally.

5.4. Recommendations

From the above conclusions, the researcher gives these recommendations.

- There is need for a law to unambiguously apply to cyber aggression or having the main two adversaries, Russia and U.S to agree on the dos and don'ts in the cyberspace.
- Russia should spearhead the formation of a military pact among Eastern Europe states and other interested states like the Warsaw Pact to counter NATO.
- An adversary will look to capitalize upon Russia's heavy dependence on technology and connectivity to achieve their ends. Therefore, it is recommended that achievable long and short term actions must be taken to protect and defend critical infrastructure.

5.5. Area for further study

- Challenges of applying deterrence theory to cyber warfare
- United States of America's cyber foreign policy
- The concept of Hybrid War

References

Adams, G. R., & Schvaneveldt, J. D. (1991). *Understanding research methods* (2nd ed.). New York: Longman.

Allen, T. S., & Moore, A. J. (Spring 2018). Victory without Casualties: Russia's Information Operations. *21st Century Political Warfare, Parameters 48 (1).*

Andrew, C., & Mitrokhin, V. (1991). *The Word and the Shield:The Mitrokhin archive and the Secret History of the KGB.* New York: Basic Books.

Appel, H. (2008). *Is it Putin or Is it Oil? Explaining Russia's Fiscal Recovery.* Post-Soviet Affairs 24 (4) : 301-323.

Babadjanov, A. (2008). "Analysis of the military doctrines of the states-participants of the CSTO". *Vestnik MGIMO- University 3*, pp. 60 - 66. Retrieved from https://elibrary.ru/item.asp?id=11689965.

Babbie, E. (1990). *Survey Research Methods* (2nd ed.). Wadsworth: Belmont.

Babbie, E. (2004). *The Practice of social research.* Belmont: CA Wadsworth Publishing Company.

Babbie, E., & Mouton, J. (2001). *The practice of social research.* Cape Town: Oxford University Press.

Babour, R. S. (1998). Mixing qualitative methods:Quality assurance or qualitative quagmire? *Quality Health Research, 8(3),* pp. 352-361.

Baldwin, D. A. (1997). The security concept. *Review of International Studies,* pp. 13.23,5-26.

Boot, M., & Doran, M. (2013). *"Political Warfare",Policy Innovation Memorandum no 33.* Washington DC: Council on Foreign Relations.

Brink, H. (1996). *Fundamentals of reserach methodology.* Cape Town: Juta and Company Ltd.

Bryman, A. (2003). *Research design in Social Research.* London: Sage.

Buchanan, B., & Sulmeyer, M. (2016). Russia and Cyber operations:Challenges and opportunities For The Next U.S Administration. *TASK FORCE ON U.S. POLICY TOWARD RUSSIA, UKRAINE, AND EURASIA.* Carnegie Endowment for International Peace.

Buzan, B., Waever, O., & Wilde, J. D. (1998). *Security: A New Framework for Analysis.* Boulder, Colorado: Lynne Rienner Publishers.

Cimbala, S. J. (2013). Russian Threat Perceptions and Security Policies: Soviet Shadows and Contemporary Challenges. *The Journal of Power Institutions in Post-Soviet Societies [Online],Issue 14/15*. doi:DOI : 10.4000/pipss.4000

Cohen, L., Manion, L., & Morrison, K. (2000). *Research Methods in Education* (5th ed.). London: Routledge Falmer.

Coughlan, S. (2003, September 30). "Is there a common understanding of what constitutes cyber warfare?". The Unversity of Birmingham School of Politics and International Studies.

Couloumbis, T., & Wolfe, J. (1990). *Introduction to International Relations:Power and Justice* (Vol. 4th Edition). New Jersey: Prentice Hall Inc.

Creswell, J. W. (2006). *Understanding Mixed methods Research.* UK: sage Publications.

Creswell, J. W. (2012). *Qualitative inquiry and research design:Choosing among five five approaches.* Thousand Oaks,CA: sage.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and Conducting Mixed methods Research* (2nd ed.). Los Angeles: Sage Publications.

Crotty, M. (1998). *The Foundations of Social Research:Meaning and Perspective in the research process.* London: Sage Publications Inc.

De Vos, A. S. (2002). *Research at grass roots* (4th ed.). Pretoria: Van Schaik Publishers.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy f Management Review Vol.14,No.4 (Oct.,1989),* pp. 532-550.

Flick, U., Kardorff, E., & Steinke, I. (2004). *A Companion to Qualitative Research.* London: Sage Publications.

Frey, F. A., Garcia, M. O., Wise, W. S., Kennedy, A., Gurriet, P., & Albarede, F. (1991). The evolution of Mauna Kea Volcano,Hawaii: Petrogenesis of tholeittic and Alkalic basalts. *Journal of Geography Research.*

Gilbert, N. (2008). *Reseaching social life* (3rd ed.). London: Sage Publications Ltd.

Griggs, B. (2008, August 18). *U.S. at risk of cyberattacks, experts say*. Retrieved September 4, 2019, from CNN News: http://edition.cnn.com/2008/TECH/08/18/cyber.warfare/index.html

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin, & Y. S. Lincoln, *Handbook of qualitative reserach* (3rd ed., pp. 105-117). Califonia: Sage.

Henning, E., Van Rensburg, W., & Smit, B. (2004). *Finding your way to Qualitative Research.* Pretoria: Schaik Publishers.

Hill, C. (2003). *The Changing Policies of Foriegn Policy.* Basingstoke: Palgrave Macmillan.

Hussey, J., & Hussey, G. (1997). *Business Research.* London: Macmillan.

Iasiello, E. J. (2017). *Russia's Improved Information Operations : From Georgia to Crimea.* Retrieved September 26, 2019, from Army War College (U.S): https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2017/8_Iasiello_RussiasImprovedInformationOperations.pdf

Jackson, T. (2011). *Ethics in Research.* London: Groombridge.

Joppe, M. (2000). *The Research Process.* Retrieved July 6, 2019, from http://www.ryerson.ca/~mjoppe/rp.html

Karaganov, S. (2011, March 4). *An iron fist to keep NATO expansion at bay*. Retrieved July 20, 2019, from Russia in Global affairs: https://eng.globalaffairs.ru/pubcol/An-iron-fist-to-keep-NATO-expansion-at-bay-15130

Kenez, P. (1995). *The birth of the propaganda state: Soviet methods of mass mobilization, 1917 - 1929.* London: Cambridge University Press.

Kerlinger, F. N. (1986). *Foundations of Behavioral Research* (3rd ed.). New York: Holt,Rinehart,Winston.

Kothari, C. R. (2004). *Research Methodology,Methods and Techniques.* New Delhi: New Age International Pvt Limited.

Kotkin, S. (May/June 2016). Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern. *Foreign Affairs.Putin's Russia*, 93(3),pp.2-9.

Koul, M. (2000). *The future of policing.* Durban, South Africa: Sage Publications.

Kuchins, A. (2005, December 26). *Moskiva na pereput'e vetrov i Vostoka*. Nezavisimaia gazeta.

Kuchins, A. C., & Zevelev, I. A. (2012). Russian Foreign Policy: Continuity in Change. *The Washington Quarterly,35:1*, pp. 147-161.

Kumar, R. (2005). *Research Methodology-A step-by-step Guide for Beginners* (2nd ed.). Singapore: Pearson Education.

Laqueur, W. (2015). The End of the Soviet Era: After Gorbachev & Who Rules Russia? : The Oligarchs. In T. Dunne, *Putinism: Russia and its Future with the West* (p. 3448). Macmillan.

Leedy, P. D. (2000). *Practical Research:Planning and Design* (7th ed.). New York: McMillan Publishing.

Light , M. (2015). Russian Foreign Policy Themes in Official Documents and Speeches: Tracing Continuity and Change. In D. Cadier , & M. Light, *Russia's Foreign Policy.* London: Palgrave Macmillan.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry.* Beverly Hills: CA:Sage.

Lukyanov, F. (2016, June). *Putin's Foreign Policy*. Retrieved August 4, 2019, from Foreign Affairs: https://www.foreignaffairs.com/articles/russia-fsu/2016-04-18/putins-foreign-policy

Maree, k., & Pieterson, V. L. (2007). First Steps in Research. In J. W. Creswell, L. Ebersohn, I. Eloff, R. Ferreira, N. V. Ivankova, J. D. Jansen, . . . C. Van der Westhuizen, *First Steps in Research Sampling* (pp. 214-223). Pretoria: Van Schuik Publishers.

Mazanec, B. M. (2015). *The Evolution of Cyberwar.* USA: University of Nebraska.

McBurney, D. (1994). *Research Methods.* California: Brooks/Cole Publishing Company.

McGuinness, D. (2017, April 27). *How a cyber attack transformed Estonia*. Retrieved October 12, 2019, from BBC News: https://www.bbc.com/news/39655415

Mcleod, J. (2001). *Qualitative Research in Counselling and Psychotherapy.* London: Sage Publications.

Mugo, F. W. (2002). *Sampling in research.* Retrieved August 26, 2019, from http://trochin.human.cornell.edu/tutorial.html

Myriam, C. (2008). *Cyber-Security and Threat Politics.* New York: Routledge.

Nygren, B. (2008). *Putin's Use of Natural Gas to Reintegrate the CIS Region, Problems of Post-Communism, 55:4, 3-15, DOI: 10.2753/PPC1075-8216550401.*

Padelford, N. J., & Lincoln, G. A. (1963). *The Dynamics of International Politics.* New york: Macmillan Company.

Pandey, P., & Pandey, M. M. (2015). *Research Methodology:Tools and Techniques.* Buzau,Romania: Bridge Centre Publishing.

Paret, P. (1989). Military Power. *The Journal of Military History vol 53, No.3*, 240.

Patton, M. Q. (2002). *Qualitative evaluation and research methods.* Thousand Oaks,CA: Sage Publications,Inc.

Polit, D. F., & Hungler, B. P. (1993). *Research Principles* (3rd ed.). Philadephia: Intervasity Press.

Pontoon, G., & Gill, P. (1993). *Introduction to politics* (Vol. 3rd World Edition). Oxford: Blackwell.

Radlin, A., & Reach, C. (2017). *Russian views of the international order.* Santa Monica: RAND.

Raulin, M. L., & Graziano, A. M. (2000). *Research Methods: A Process of Inquiry.* Boston: Allyn and Bacon.

Rowe, A. (2019, June 19). *Russia Taunts US with Threat of Cyber War*. Retrieved October 2, 2019, from Tech.Co: https://tech.co/news/russia-taunts-us-with-threat-of-cyber-war-2019-06

Sanger, D. E. (2012). *Confront and Conceal:Obama's Secret Wars and Surprising Use of American Power* (Kindle Edition ed.). Broadway Books.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students* (4th ed.). Edinburgh Gate,Harlow: Financial Times Prentice Hall.

Schmidt, M., & Sanger, D. (2015, April 26). *Russian Hackers Read Obama's Unclassified Emails, Officials Say*. Retrieved September 28, 2019, from The New York Times: https://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html

Segal, A. (2016). *The Hacked World Order: How Nations Fight,Trade,Maneuver, and manipulate in the Digital Age.* New York: Public Affairs.

Shevtsova, L. (2002). Power and Leadership in Putin' s Russia. In A. C. Kuchins, *Russia after the fall* (pp. 62-78). Washington, DC: Carnegie Endowment for international Peace.

Singer, P., & Friedman, A. (2014). *Cybersecurity:What Everyone Needs to Know.* US: Oxford University Press.

Singh, A. S., & Masuku, M. B. (2014). 'Sampling Techniques and Determination of Sample size in Applied Statistics and Research: An Overview'. *International Journal of Economics,Commerce and Management, Volume ll(11)*, 1-22.

Smith, D. J. (2014, January 17). *Russian Cyber Strategy and the War Against Georgia*. Retrieved September 5, 2019, from Atlantic Council: https://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia/

Softa, J. (2008). *Threats Against Russia's Information Society.* Charleston: S.C.:BookSurge.

Soldatov, A., & Borogan, I. (2015). *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries.* New York: Public Affairs.

Stake, R. (1995). *The art of case study research.* Thousand Oaks,CA: Sage.

Thomas, T. L. (1998). "Dialectical versus Empirical Thinking:Ten Key Elements of the Russian Understanding of Information Operations". *Journal of Slavic Military Studies 11 no.1,* 40-62.

Thomas, T. L. (2015). *Russia military strategy: Impacting 21st century reform and geopolitics.* Fort Leavenworth,Kan: Foreign Military Studies Office.

Unwala, A., & Ghori, S. (2015). Brandishing the Cybered Bear: Information War and the Russian-Ukraine Conflict,". *Military Cyber Affairs 1, no. 1.: doi:10.5038/2378-0789.1.1.1001*.

Vijay, S., Hoikka, H., & Blomqvist, K. (2016). *Ukraine 2015 Power Grid Cyber Attack-ELECT-E7470 Cybersecurity L-Case Study Group.* Cyber Warriors.

Vorobyov, I., & Kiseljov, V. (2013). Russian Military Theory : Past and Present. *Military Thought (3)*.

Waltz, K. (1979). *Theory of International politics.* Boston: Mcgraw Hill.

Webber, M., & Smith, M. (2002). *Foreign Policy in a Transformed World.* London: Prentice Hall.

Wegner, D. M. (2002). *The illusion of conscious will.* Cambridge,MA,US: MIT Press.

White, S. P. (20 March 2018). *Understanding Cyberwarfare: Lessons from the Russia-Georgia war.* At West Point: Modern War Institute.

WhiteHouse. (2009, May 29). *Remarks by the President on Securing Our Nation's Cyber Infrastructure*. Retrieved September 6, 2019, from Obama Whitehouse: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Wingfield, T. C. (2000). The Law of Information Conflict: National Security Law in Cyberspace. *Aegis Research Corp*, 17.

Winter, G. (2000). *A comparative discussion of the notion of validity in qualitative and quantitative research.* The Qualitative Report,4(3&4).

Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Elsevier: Inc Waltham.

Wirtz, J. J. (2015). "Cyber War and Startegic Culture: The Russian Intergration of Cyber Power into Grand Strategy. In K. Geers, *Cyber War in Perspective:Russian Aggression Against Ukraine* (p. 31). Tallinn: NATO CCD COE Publications.

Wolfers, A. (1952). "National Security" as an Ambiguous Symbol. *Political Science quarterly,67*, p. 4.

Yin, R. K. (1994). *Case Study Research:Design and Methods* (2nd ed.). London: Sage Publications.

Zvekic, U. (2000). Criminal Victimisation in Countries in Transition. Rome: UNICRI Publication.

Appendix A

RESEARCH TITLE

Cyber warfare as a new threat to security policy: A Russian foreign policy perspective.

RESEARCHER

Mr. E. Mugwira
Department of Peace and Governance. Bindura University of Science Education

Introduction

Mugwira Edwin is a student at Bindura University of Science Education pursuing a Master of Science in International Relations degree programme. As part of his dissertation in partial fulfillment of the requirement for the Master of Science in International Relations degree programme, Edwin is carrying out a research. Please note that this research is purely for academic purposes. Your response will be treated with a high degree of confidentiality and at all-time data will be presented in such a way that your identity cannot be connected with specific published data.

Instruction

Please answer as honestly as you may. If you feel any question is uncomfortable to you, please inform me and we will proceed to the next question. You may terminate this interview at any time.

SECTION A - RUSSIAN FOREIGN POLICY AND NATIONAL SECURITY

How can you describe the Russian foreign policy?

Has Russia used cyber tactics to win wars?

Can Russia be regarded as a passive or aggressive state in cyber-attacks?

How is Russia implementing its cyber tactics?

SECTION B - ROOTS OF RUSSIAN CYBER POLICY

When did cyber warfare become dominant?

What is shaping the Russian cyber warfare policy?

Can cyber warfare influence security policy? If yes how?

Are states giving this new threat of cyber-attacks enough attention?

SECTION C – HOW STATE ACTORS RESPONSE TO RUSSIAN CYBER-ATTACKS

Which part of the globe is cyber warfare more prevalent?

Can having cyber capabilities be equated to nuclear possession?

Is everyone susceptible to cyber-attacks?

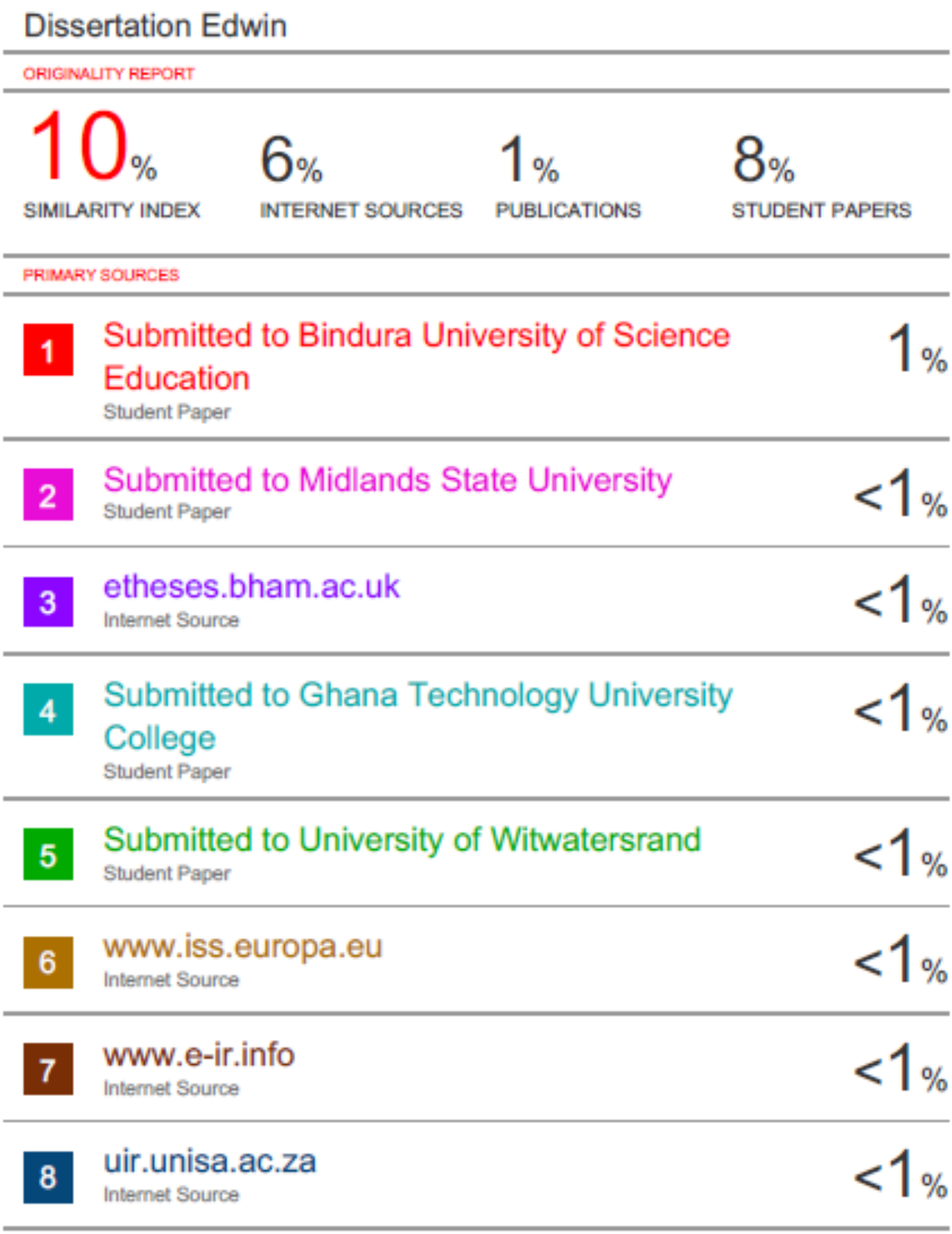
Who are the most vulnerable to cyber-attacks?

How can state actors prevent themselves falling victims of cyber-attacks?

Can a state recover from cyber-attacks?

This is the end of the interview. Are there any questions that you would like to ask? If not, thank you for your participation.

Antiplagiarism Report



Dissertation Edwin

ORIGINALITY REPORT

10%	6%	1%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Bindura University of Science Education Student Paper	1%
2	Submitted to Midlands State University Student Paper	<1%
3	etheses.bham.ac.uk Internet Source	<1%
4	Submitted to Ghana Technology University College Student Paper	<1%
5	Submitted to University of Witwatersrand Student Paper	<1%
6	www.iss.europa.eu Internet Source	<1%
7	www.e-ir.info Internet Source	<1%
8	uir.unisa.ac.za Internet Source	<1%