THE INVISIBLE BATTLEFIELD: ANALYZING CYBERSECURITY THREATS AND THEIR IMPLICATIONS ON ETHIOPIAN NATIONAL SECURITY (2013-2023)

BY:

MENGESHA FENTAW

JULY, 2024

ETHIOPIA

ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

INSTITUTE FOR PEACE AND SECURITY STUDIES (IPSS)

The Invisible Battlefield: Analyzing Cybersecurity Threats and Their Implications on Ethiopian National Security (2013-2023)

BY:

Mengesha Fentaw

A thesis paper submitted to the Institute for Peace and Security Studies for The Partial fulfillment of the requirements of Master of Arts in Peace and Security Studies at Addis Ababa University

Advisor:

Yohannes Tekalign (PhD)

July, 2024

DECLARATION

I hereby declare that this thesis is the outcome of my independent research, unless stated otherwise. Throughout this study, I have conducted my investigation autonomously, under the guidance and support of my research advisor. Any external sources used have been duly acknowledged through citations with clear references.

Mengesha Fentaw

Signature: _____

APPROVAL

This thesis, entitled "The Invisible Battlefield: Analyzing Cybersecurity Threats and Their Implications for Ethiopian National Security (2013-2023)" by Mengesha Fentaw, is recommended for acceptance by Addis Ababa University in partial fulfillment of the requirements for the Master of Arts Degree in Peace and Security Studies. It has been examined and approved by the undersigned, who certify that it complies with the university's regulations and meets the standards of originality and quality expected of scholarly work.

Advisor: Yohannes Tekalign (PhD)
Signature: _____
Date: _____

Name of Internal Examiner: Fana Gebresenbet (PhD)
Signature: _____
Date: _____

Name of External Examiner: Amare k. Aweke (PhD)
Signature: _____
Date: _____

Name of Head of Department: _____
Signature: _____
Date: _____

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to Almighty God for granting me the strength and determination to complete this thesis.

I am sincerely thankful to my advisor, Dr. Yohannes Tekalign, for his exceptional guidance, unwavering support, and motivation during this research journey.

I extend my appreciation to the leaders, members, and colleagues at the Information Network Security Administration (INSA) for their continuous support and collaboration.

Additionally, I am grateful to the leaders, members, and colleagues at the Ethiopian Defense Force Cyber Directorate, the Ethiopian Defense University, and the Ethiopian Air Force for their valuable contributions and assistance, which significantly influenced the success of this research.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

This thesis investigates the evolving landscape of cybersecurity threats in Ethiopia over the past decade, elucidating the underlying factors and assessing their impact on national security. A mixed-methods research approach was employed, integrating quantitative data analysis with qualitative insights from open interviews to provide a comprehensive understanding of the issue. The findings of the analysis showed that the data obtained from multiple sources indicated a significant escalation in both the frequency and sophistication of cybersecurity threats, posing an increasing challenge to Ethiopia's cyber resilience. Key contributing factors were identified as insufficient cybersecurity infrastructure, dependency on foreign technology, outdated or inadequate cybersecurity policies, local political dynamics, and geopolitical tensions. These factors collectively amplify the severity of the cyber risk confronting the nation. These findings further underscore the critical implications of cybersecurity threats to Ethiopian national security. Manifestations of these threats include disruptions to critical infrastructure, adverse effects on political stability, and compromises to national sovereignty due to recurrent nation-state cyber-attacks.

Keywords: Cybersecurity Threats, National Security, Foreign Technology Dependency, Cybersecurity Policies, Political Dynamics, Cyber-Attacks, Critical Infrastructure, National Sovereignty.

Chapter One

Introduction

1.1 Background of the Study

Computer technology has become essential for solving various problems in the contemporary digital era. However, the rapid advancement of this technology has posed a significant security threat through cyberattacks (Skopik, 2018). Cyberattacks have recently targeted critical infrastructure, causing extensive damage and disruption (Sharma, 2010). These attacks have also led to theft of vital information, jeopardizing national security (Alsamadi, 2019; Goel, 2020). Furthermore, these attacks have contributed to the escalation of political instability as they can be used to manipulate or influence political outcomes (Alsamadi, 2019). According to Sun Tzu, a famous ancient Chinese military strategist, the true skill in warfare lies in defeating the enemy without direct combat. In the 21st century, this concept of strategy has applied in cyberspace, where states and non-state actors use cyber weapons to disrupt their adversaries' critical infrastructure without physical confrontation. Cyber-attack on Iran's nuclear reactor is an example of this form of warfare, highlighting the need for improved cyber-security measures to protect national security (Sharma, 2010).

Ethiopia is facing a growing threat of cyberattacks from foreign powers as it pursues its technology development goals (Alemayehu, 2023). These attacks have disrupted the online services of the private and government sectors, including the Grand Ethiopian Renaissance Dam (GERD), which is a source of tension with Egypt and Sudan over Nile water shares (Elsa, 2023). To address escalating cybersecurity threats effectively, Ethiopia has established cybersecurity institutions such as INSA and implemented policy measures. However, scholars argue that these efforts may be insufficient and outdated (Halefom, 2015; Iyasu, 2018; Yirga, 2022).

This study investigated the impact of rising cybersecurity threats on Ethiopia's national security using a mixed-methods research approach within an explanatory sequential research design. It analyzed the historical trends of cybersecurity threats in Ethiopia over the past decade, explored factors contributing to their escalation, and evaluated their implications for national security.

1.2 Statement of the problem

Internet coverage and digitalization in Ethiopia have been rapidly growing, contributing to the countrys development and poverty reduction (Misgana, 2021). The government is also working on a digital strategy that will be fully operational by 2025 (Khalid, 2021). However, this rapid increase in digitalization has made Ethiopia highly vulnerable to cyberattacks, posing a threat to its national security (Kumar, 2022; Markos, 2022). According to the Ethiopian Monitor (2023), the country has experienced cyberattacks from various sources, including states, non-state actors, and state-sponsored groups, targeting its government, military, media, and critical infrastructures. These attacks have significantly challenged Ethiopian national security (Ethiopian News Agency, 2022; Fana Broadcasting Corporate, 2023).

The main problem this study addresses is the lack of a comprehensive and systematic analysis of the implications of cybersecurity threats on Ethiopian national security. Existing studies focus on specific aspects of cyberattacks, such as legislative measures (Halefom, 2015; Knife, 2016; Temesgen, 2019) and policies (Abenezer, 2019), but there is no integrated assessment of how these threats impact national security. Additionally, the factors behind the increase in cybersecurity threats have not been clearly identified.

If this issue is not addressed, Ethiopian national security policies and strategies will remain inadequately informed and potentially ineffective, leaving the country vulnerable to escalating cyber threats. By systematically examining the level of cybersecurity threats, identifying contributing factors, and analyzing how these threats affect national security, this study aims to provide the comprehensive understanding needed to enhance security policies and strategies. This will enable the government to make timely adjustments, ensuring policies are effective in mitigating cybersecurity threats and protecting national security.

1.3 Objectives

1.3.1 General Objective:

The general objective of this study is to comprehensively analyze the evolution and trends of cybersecurity threats in Ethiopia over the past decade and systematically assess their implications for national security.

1.3.2 Specific Objectives:

The following are the specific objectives of the study

1. To analyze the evolution of cybersecurity threats in Ethiopia over the past decade (2013 – 2023).
2. To assess the primary factors that have significantly contributed to the escalation of cybersecurity threats in Ethiopia.
3. To examine the implications of cybersecurity threats on Ethiopia's national security, examining how these threats influence and shape the overall security of the country.

1.4 Research Questions

The study attempts to answer the following key questions

1. What changes occurred in the trend of cybersecurity threats in Ethiopia over the past decade?
2. What factors significantly contribute to the rise of cybersecurity threats in Ethiopia?
3. How do cybersecurity threats impact the overall national security landscape in Ethiopia?

1.5 Significance of the Study

Because the study highlights the state of cybersecurity threats in Ethiopia, identifies the specific factors behind these threats, and examines how cybersecurity threats impact national security, it is particularly important for government policymakers. The public also benefits from this study, as it raises awareness of emerging threats in cyberspace. In addition, this study contributes to the academic field of cybersecurity, especially for researchers who need to study it in terms of national security.

1.6 Scope of the study

The scope of this research was limited to cybersecurity experts currently working in the field of cybersecurity in Ethiopia. The study particularly targets government cybersecurity officers, with the majority (83%) of the participants being from government agencies. A smaller proportion (17%) included private cybersecurity experts.

1.7 Delimitation of the Study

The study's delimitations originated primarily from the relatively small number of participants due to the shortage of cybersecurity experts, particularly in the private sector, and the sensitivity

of the data related to cybersecurity and national security, as a large portion of cybersecurity and national security data are highly classified and sensitive. As a result, including all relevant data in this study is challenging. Furthermore, certain factors were excluded from this study to narrow its scope.

1.8 Organization of the paper

This paper is organized into six chapters. Chapter one highlights the background; Chapter two explains the related literature review and conceptual framework of the study. Chapter three illustrates the research methodology; Chapter four focuses on data presentation; Chapter five includes data analysis and key findings; chapter six includes the conclusion and limitations of the study; and the final sections of the study present references and appendices.

Chapter Two

Review of Related Literature

2.1 Introduction

The purpose of this literature review is to offer a comprehensive examination of the current literature and to understand the surrounding cybersecurity and its implications for national security, particularly within the context of Ethiopia. The literature review explored a wide range of sources, including academic articles, research papers, and government reports, to gather a holistic understanding of the subject matter. By analyzing these sources, the review identified the key themes, theories, and empirical evidence that have been examined in relation to cyber security threats and national security. Furthermore, the literature review identified gaps and limitations in the current literature. The literature review is organized into five main sections: an overview of the chapter, conceptual clarification of terms and concepts, theories regarding cybersecurity and national security, empirical literature, and the conceptual framework.

2.2 Conceptual Clarifications

2.2.1 The Concept of Security

The concept of security is ambiguous and, as a result, various scholars have defined it differently. However, after the end of the Cold War, vagueness increased considerably, owing to the rise of new paradigms. Buzan (1997) states that scholars should define the concept of security with further clarification, as many researchers are not interested in exploring it because of its vagueness and the rapid technological and political changes that characterize the security environment.Arnold Wolfers was one of the few scientists who attempted to define the concept of security. He formulated that security can be defined in two different ways: "objectively as the absence of threats to acquired values" and "subjectively as the absence of fear that those values will be attacked" (Wolfers, 1952, p. 485). Buzan and Hansen (2009) provide a detailed explanation of the different epistemological perspectives on security. They note that objective views of security often, but not always, focus on material aspects, such as the ability of states to pose threats or deter enemies based on their material capabilities. In contrast, subjective views emphasize the roles of history, norms, psychological factors like fear and misperception, and the relational contexts involving friends, rivals, neutrals, and enemies in shaping security threats.

Additionally, discursive approaches contend that security cannot be objectively defined, making both objective and subjective views potentially misleading. Furthermore, David A. Baldwin suggested two questions to define security more clearly: "Security for whom?" and "security for which values?" According to this concept, security has two main dimensions: the traditional one, which deals with the security of states against military threats, and the non-traditional one, which covers the security of other actors against non-military threats (Baldwin, 1997).

2.2.1.1 The concept of national security

The concept of national security has been reshaped by globalization, as it has increased the range and intensity of threats that states have faced in the 21st century (Andy, 2010). Wolfers (1952) defines national security as the ability of a government and its parliaments to safeguard the state and its citizens against all sorts of "national" crises by using various power projection strategies, including diplomacy, economic power, and military power. Similarly, Lippmann (1943) argued that the national security of a state relies on its ability to safeguard its fundamental values from foreign threats. Some authors define national security as the pursuit of security for a state in an unsecured world (Kegley et al., 1985: 371). Another scholar also stated national security as "the capacity to maintain the physical integrity and territory of the nation, to preserve its economic relations with the rest of the world on reasonable terms, to protect its nature, institutions, and government from outside interference, and to control its borders" (Berouk, 2002, p.14; Brown, 1983, p. 4).

2.2.1.2 National security for Ethiopia

National security is the top priority of Ethiopia's foreign and security policy. This is evident from the document entitled "Foreign Affairs and National Security Policy and Strategy," which states:

> *In a fundamental sense, security policy is a matter of ensuring national survival. The Alfa and omega of security is ensuring national survival. Other questions of national security can only be asked if national existence is secured. Foreign and security policy must be formulated first and foremost to ensure national security. Issues of prosperity, lasting peace, stability, and other related concerns will then follow. (Ministry of Information, 2002).*

The current Ethiopian national security policy prioritizes domestic affairs over external ones, identifying poverty, backwardness, and a lack of good governance as the primary threats to national existence. This policy criticizes the previous national security framework for its predominant focus on external rather than internal issues. It emphasizes that external threats are often linked to internal challenges or exploit vulnerabilities caused by internal difficulties (Ministry of Information, 2002). Although this policy is under revision and a new foreign policy has been drafted, it remains the widely recognized national security policy in Ethiopia.

2.2.2. Cybersecurity and Related Concepts

Regarding cybersecurity and related terms such as cyberspace and information security, countries around the world provide different definitions based on their own context. According to Abenezer (2019), various states, institutions, and scholars have defined cybersecurity terms based on their interests and perspectives. Consequently, finding a universally accepted definition for such terms is challenging. In this section, the definitions of some specific cybersecurity terms that are most commonly used in this study are presented.

Cybersecurity and Information Security

Most cybersecurity strategies and policies in different countries define cybersecurity as the safeguarding of cyberspace against cyber threats. However, some countries, such as Austria and Finland, limit the scope of cybersecurity to protecting digital information or critical infrastructure from cyber threats. For others, it is about combating any type of cyber assault in cyberspace. These different perceptions regarding cybersecurity have led to various methods of combating and minimizing cyber incidents (Shafqat & Masood, 2016, p. 27).

In the Ethiopian context, the terms cyber security and information security are mostly used interchangeably, and the Ethiopian Information Security Policy of 2011 defines information security as "the protection of information from attacks that eradicate its integrity, confidentiality, and availability during collection, processing, storage, and transmission; however, some scholars differentiate them by defining information security as the protection of information assets in any form, whether physical or not, and cyber security as the protection of information and non-information assets within the ICT infrastructure (von Solms & van Niekerk, 2013).

Cyberspace

Ethiopia defined cyberspace in the 2011 Ethiopian National Information Security Policy as "a global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunication networks, computer systems and embedded processors and controllers."

Cyberwar and Cyber-attack

NATO defines cyberwar as a state of conflict in which nation-states use cyberattacks against the ICT systems of critical infrastructure as part of their military strategy (NATO CCDCOE, 2016). Lewis (2013) distinguishes between cyberwar and cyber-attack, concepts that are further discussed by Hughes (2017). According to Lewis, cyberwar refers to the use of cyber techniques by states or political groups to cause damage, destruction, or loss for political purposes. A cyberattack, on the other hand, is a single act aimed at causing damage, destruction, or casualties in cyberspace. According to Ethiopian Information Network Security Agency Re-Establishment Proclamation No. 808-2013 Cyber-attacks include "the destruction of computer-based critical infrastructures or the disruption of their services, or obliterating the confidentiality, integrity, or availability of information, computer-based psychological attacks on citizens, or digital identity theft perpetrated by different techniques." (FDRE, 2014).

Critical Infrastructure

According to INSA re-establishment proclamation no. 808-2013, "critical infrastructure is an infrastructure that can have considerable damage to public safety and the national interest if attacked." (FDRE, 2014).

2.3 Theories on National Security and Cyber-security

Although there are several cybersecurity theories and models, this study focuses on specific theories that intersect with cybersecurity and national security. This section addresses international security theories that allow us to determine cybersecurity and its implications for national security, with emphasis on Ethiopia's cybersecurity landscape.

Liberalism

According to liberalism, various players besides the state play an important role in the international system. This approach aims to promote peace and stability between governments

and stakeholders through collaboration and consensus. Richmond (2009) described liberalism as a tradition that prioritizes international collaboration and acknowledges the significance of nonstate actors (Oneal & Russett, 1996).

According to liberal theory, cyber hostilities are improbable among democratic states, which mostly engage with and target non-democratic states in cyberspace as part of their conventional war strategy. Liberalism also argues that the state alone cannot ensure cybersecurity and that international cooperation between states and corporations is required to secure cyberspace. Therefore, according to this theory, to achieve cyber security globally, various international agreements at the bilateral and multilateral levels are necessary (Isnarti, 2016; Falk, 2002).

Some researchers believe that adopting liberalist cybersecurity principles may benefit Ethiopia's national security. Regarding Ethiopia's preliminary stages in building cyber-defence capabilities, the liberalist approach to international collaboration and information exchange is likely to be helpful to gain substantial experience in the complicated arena of cybersecurity (Yabets, 2022; Misgana, 2021). However, Ethiopia is far from adopting liberal cybersecurity concepts. The country has never engaged in international or regional cybercrime initiatives nor has it collaborated on a worldwide scale to combat cybercrime (Iyasu 2018). Furthermore, Ethiopia hasn't joined the "African Union Convention on Cyber Security and Personal Data Protection," which has been regarded as a significant step in standardizing legislative and regulatory standards for cyber security all over the continent (Yabets, 2022; Misgana, 2021).

One critique of liberalism in cyber conflict is that it is excessively optimistic about the prospects of international collaboration in securing cyberspace. Liberalism considers cyberspace as a by-product of the liberal system, and liberal ideals and institutions promote peace and security in this domain. However, this assumption neglects the fact that cyberspace is a disputed domain with diverse interests, values and competencies. As a result, despite liberal optimism, we cannot be confident that global agreements and institutions will successfully address cyber conflict. Furthermore, liberalism provides insufficient knowledge and arguments on how liberal norms and institutions would operate effectively in this domain (Isnarti 2016). Liberalism falls short of describing the cybersecurity landscape in Ethiopia because, according to various sources, the country is experiencing a high-risk state-sponsored cyberattack on its critical infrastructure and core values at the national security level.

Realism

Realism theory is based on three fundamental assumptions that describe how nations react to the international system. The assumptions are as follows: 1) states are the principal actors in the global system, 2) they seek and prioritize their interests, and 3) the international system is anarchic. According to this perspective, states can employ military force as the last option to confront prospective adversaries or enforce their will on others. This can entail both physical attacks and deterrents (Jorge 2012).

Realist theorists believe that cyberspace lacks effective international regulations. The Internet, which constitutes a vital part of cyberspace, has emerged in a decentralized manner without a single global entity in charge of its administration (Tabansky, 2011). As a result, cyberspace exhibits an anarchic condition, meaning that there is no authority above states that can enforce their will on them in the cyber domain (Kremer & Müller, 2014). This situation reflects the broader realist perspective of international relations as a system dominated by self-interest and power, rather than global norms and rules. Reardon and Choucri (2012) argue that realist theories of international relations are relevant for understanding cyber security in the international arena; furthermore, realism theories can illuminate how states employ cyber technologies to enhance their security interests and how they react to other states the cyber capabilities.

Realism is the most relevant theory to understand the current status of cybersecurity in Ethiopia and its implications for national security for various reasons. First, in realism, the main focus is the survival of the state; in the policy of "Ethiopian national security and foreign affairs," the survival and well-being of the country hold priority over other matters. Second, Ethiopia has recently experienced state-sponsored cyberattacks against its critical infrastructure and core values by foreign states to fulfill their own interests (Yirga, 2022). This reflects the realist notion that states always act according to their own interests regardless of the harm caused to others. Third, while Ethiopia is experiencing multiple state-sponsored cyber-attacks, international institutions have not interfered, and not even with the African Union's cybersecurity department. Through the lens of realism, this demonstrates the true anarchic nature of cyberspace. Fourth, cyberspace is already globally militarized, particularly in the Ethiopian context. In this case, Ethiopia officially labeled cyberspace as the domain of warfare, in addition to land, air, and sea. Furthermore, Ethiopian officials have repeatedly stated that Ethiopian adversaries are trying to

violate the country's sovereignty in cyberspace. Moreover, since the main objective of this study is to analyze the cybersecurity threat and its implications for Ethiopian national security, the theory of realism is more relevant than other theories.

Liberals criticize realism for neglecting the diverse actors in cyberspace, such as non-state actors, hackers, terrorists, and civil society groups. They also question the ability of realism to deal with cyber terrorism, a major global security threat. Furthermore, they challenge realism's assumption of power in cyberspace, which is difficult to measure and varies across actors. For example, the U.S., a conventional great power, is often exposed to cyberattacks from weaker states or non-state actors. Liberals argue that realism cannot account for the power dynamics in the international cyber system, nor can it map the cyber power distribution among various actors (Isnarti, 2016).

Cybersecurity Dilemma

The cybersecurity dilemma is the concept that states may unintentionally threaten the security and stability of other states by intruding into their vital networks to protect their own cybersecurity. This concept is based on the security dilemma, which explains how states' self-defence actions can cause fear in other states. In cyber security, states may launch intrusions early to gain offensive advantages or prevent other states from intruding into their networks. States must worry about both visible and invisible threats in cyberspace. Even peaceful states are subject to a security dilemma, as they must ensure their safety in a risky world (Buchanan, 2016, p. 3).

2.4 Empirical Literatures

This section examines empirical studies of the complex web of cybersecurity threats and their profound impact on national security. Starting from a global and African context, Ethiopian cybersecurity status in particular is highlighted, and existing academic works dealing with Ethiopia's cybersecurity landscape are critically reviewed.

2.4.1 Cybersecurity and National Security: A Global Perspective

As cyber adversaries develop new techniques, tools, and strategies to exploit vulnerabilities and weaknesses, the global landscape of cyberattacks is constantly evolving (Goel, 2020). Recently, a notable shift has occurred in cyber-attacks. While cybercriminals and hackers used to be the

main perpetrators, countries now also use cyber-attacks to pursue their own national interests. Their goal is to paralyze perceived enemy states, which results in the emergence of cyber war as a significant threat (Goel, 2020). In response to this threat, many countries worldwide have adopted the term ‘cyber war’ in their military strategy and doctrine (Ülgen, 2016). This emergence of cyber war poses a significant danger to national security, as it has the potential to disrupt critical infrastructure, steal sensitive information, distort political stability, and interfere with internal affairs (Clarke & Knake, 2010; Kim, 2011). The following cases indicate the risks posed by cybersecurity threats to national security:

Cyber War against Estonia

In 2007, Estonia experienced a difficult and extensive cyberattack that lasted 22 days. The attacks were part of a broader political dispute between Estonia and Russia over the removal of Tallinn-era monuments (Ottis, 2008). In these cyber-attacks, websites were defaced and false propaganda spread via social media. The attacks had an impact on daily life, the economy, fundamental values, and the image of the country. This politically motivated cyber-attack is considered one of the indicators of the emergence of cyberwar in the 21st century and has triggered great awareness in the international community regarding cybersecurity threats and their impact on national security (Valenta & Valenta, 2018).

The Cyber-attack against Iran’s Nuclear Facility

The U.S. and Israeli intelligence services are believed to have created Stuxnet malware, which attacked the Natanz nuclear facility in Iran. It penetrated the facility’s industrial control systems and caused centrifugal malfunction, while showing normal readings to the operators. This cyber operation aimed to slow down Iran’s nuclear weapons program without physical attack. Stuxnet was important because it was the first known case of a cyber-operation that caused physical damage outside a controlled testing environment. This shows the potential effectiveness and value of cyber-weapons. The incident also showed that cyber warfare can be a serious threat to national security by allowing attacks that can cause physical harm or disrupt critical infrastructure (Lachow 2011).

2.4.2 Cybersecurity threats in Africa

Africa has been labeled a safe haven for cybercriminals, largely because it has failed to do more to combat the threat (Eboibi, 2020). Africa is particularly vulnerable to cybersecurity threats

owing to the rapid development of digital technology and lack of sufficiently strong cybersecurity measures. (Mathe, 2019; Kibreab, 2020). While cybercriminals target African countries from inside and outside the continent, most African countries lack the technological and economic capacity to detect and monitor critical online activities that are critical for national security (ECA, 2014). Consequently, cybersecurity threats in Africa escalated.

2.4.2.1 African Union Convention on Cyber Security and Personal Data Protection

Due to the escalating threats associated with cyberspace and the challenges posed by rapid digitalization, the AU has acknowledged that cybercrime is one of the greatest challenges Africa will face in the twenty-first century (Iyasu, 2018, p.38). As a result, "A Convention on Cyber Security and the Protection of Personal Data" was adopted in June 2014. This convention reflects African countries' commitment to the development of an information society at the sub-regional, regional, and international levels. The document recognizes the continued protection of fundamental freedoms and human rights, as expressed in several declarations and international documents adopted by the AU and the United Nations. In addition, the Convention aims to address the need for harmonized cybersecurity legislation in member countries and recognizes that cybercrime poses a real threat to the security of computer networks and the progress of the information society in Africa. One of the objectives of the Convention is to prevent double criminality. To achieve this, countries are encouraged to sign mutually beneficial treaties and ensure that their efforts to combat cybersecurity threats are regionally coordinated, as well as that they are responsible for developing national cybersecurity strategies and protecting their national security from cybersecurity threats.

The Convention has been criticized for its broad scope, which goes beyond cyber-security-related issues, and attempts to cover a wide range of issues (including the protection of personal data and electronic transactions) that require specific legislation in a single instrument (Iyasu, 2018). Furthermore, the Convention has been criticized for failing to establish a regional supervisory body, rather than simply encouraging states to cooperate and collaborate. In my view, the Convention failed to address current cybersecurity challenges, especially in the context of state-sponsored cyber-attacks and the militarization of cyberspace, which have escalated tensions among states.

2.4.3 Cyber security threats and National Security: The Case of Ethiopia

2.4.3.1 Digital and cyber-security landscape of Ethiopia

Ethiopia has a large population of 125 million people, but a low Internet penetration rate of 16.7 percent relative to similar developing countries and only 20.86 million people had access to the Internet in January 2023. The number of Internet users increased by 520 thousand (+2.6 percent) from 2022 to 2023, but this growth rate was still slower than that in other African countries. Ethiopia ranks among the ten least ICT developed countries in Africa (Kemp, 2023). According to Alemayehu (2022), Ethiopia has a very low level of digitalization advancement compared to other countries in the region. Even if digitalization in some sectors, such as the financial industry, is rapidly increasing, it still ranks lowest regarding regional standards.

Regarding cyber-attacks against Ethiopia, various local and external sources present varying data; however, all sources present exponential growth in cyber-security threats. According to the global cyber-security company Kaspersky, the company’s data analysis showed that Ethiopia faced about 18,000 cyber-attacks and 30,000 ransom ware incidents in 2023 (Capital Newspaper, 2023, June 12). The Ethiopian cyber security audit and evaluation directorate Tilahun Ejegu stated that “cyberattacks against Ethiopian critical infrastructure have increased from 214 to 8845 in the past five years” (Ethiopian News Agency, 2023). Furthermore, based on Security Magazine 2020, Ethiopia is the third country most exposed to cybersecurity threats globally, and the first in Africa and Business Insider Africa in 2023, Ethiopia was the third most vulnerable country to cybersecurity threats in Africa (Table 5).

2.4.3.2 Cyber security threats and Its Implications for Ethiopian National Security

Ethiopia is becoming a victim of cyberattacks as a result of rapid technological changes, as well as various geopolitical and domestic factors, and escalating attacks have become a threat to national security. Since drafting a cyber-security policy in 2011, the Ethiopian government has taken a variety of measures in response to the escalation of cyber-attacks on critical sectors. The third National Cyber Security Month, held in October 2022, commenced with the theme "Integrated Cyber Security for National Sovereignty." During this event, Deputy Prime Minister and Minister of Foreign Affairs, Demeke Mekonnen, emphasized the importance of cyber technology for the country's success, stating that the government has prioritized the sector as a

strategic focus in its 10-year development plan. Consequently, the government is addressing cyber security as a critical national security issue (Fana Broadcasting Corporation, 2022). Professor Birhanu Nega, Minister of Education, also states that "everyone should take the necessary precautions to avoid such attacks and make efforts to learn more about cyber security. Otherwise, cyberattacks will pose serious threats to the country's national security" (Walta Information Center, 2021).

2.4.3.3 State sponsored cyber-attacks against Ethiopia

Cyber-war attempts against Ethiopia intensified after the filling of the Renaissance Dam, which the Ethiopian government claimed was met with various cyber-attacks sponsored by Egypt. A menacing message appeared on many hacked Ethiopian government websites on June 19 and 20, 2020, along with the image of a skeleton pharaoh. The message read: "If the river's level drops, let all the Pharaoh soldiers hurry and return only after the liberation of the Nile, restricting its flow. To prepare the Ethiopian people for the wrath of the Pharaohs." The Ethiopian Information Networks Security Agency (INSA) announced that it had removed the images and texts, but the websites remained offline until June 27 (Ethiopian Press Agency, 2020). The Ethiopian government also claimed that many external actors were involved in cyber-attacks against the Grand Ethiopian Renaissance Dam (GERD). According to Samme-Nlar (2020), recent cyberattacks against Ethiopia are indicators of future cyber conflicts in Africa.

2.4.3.4 Political dynamics and cybersecurity threats in Ethiopia

Political unrest in the country has also aggravated cybersecurity threats. For example, Ethiopia faced various external political pressures and cyber-attack attempts after the Tigray War (OHCHR & EHRC, 2021). There are indications that large-scale cyberattacks against Ethiopia are related to both internal and external political issues. Dr. Shumete Gizaw (2021), Director-General of the Information Network Security Agency (INSA), stated that cyber-attack attempts have increased in Ethiopia. This surge is particularly connected to significant national events such as the second filling of the Grand Ethiopian Renaissance Dam (GERD), the sixth general elections, and the law enforcement operation in the country's north. These events are highly sensitive and critical, making Ethiopia more vulnerable to cyber threats. The increase in cyberattacks during these periods reflects the heightened political tensions and strategic

importance of these events, which adversaries may seek to exploit. Furthermore, Cyber-attack attempts have been increasing in Ethiopia, particularly in connection with the second filling of the Grand Ethiopian Renaissance Dam (GERD), the six general elections, and the law enforcement operation held in the northern part of the country (Ethiopian News Agency, 2021).

2.4.3.4 The Institutional Landscape of Cybersecurity in Ethiopia

A Brief Overview of Ethiopia's Cybersecurity Institutions

To combat the escalated cybersecurity threat, Ethiopia has taken various institutional measures. The following Ethiopian institutions have the duty to deal with cybersecurity:

• The Information Network Security Agency (INSA), which was re-established in 2013, reports to the Prime Minister. It is responsible for developing and implementing national cybersecurity policies, standards, and strategies, as well as securing vital information infrastructures and regulating cryptographic products and transactions (The Federal Negarit Gazzete, 2014; Abenezer, 2019).

• The Federal Police Cyber Unit Division, established in 2004 with the support of the American FBI. It is in charge of cybercrime investigations in the country with technical support and training from the INSA. However, it still faces challenges in effectively addressing cybercrime (Abenezer 2019).

• The National Intelligence and Security Service (NISS), which was re-established in 2013 and reported to the Prime Minister. It is the main agency that leads to intelligence and security services in Ethiopia. It fights cybercrime both inside and outside the country, issues directives and standards for the protection of critical institutions, follows up on threats to economic security, and collects and provides necessary data to the relevant bodies (The Federal Negarit Gazette, 2013; Abenezer, 2019).

• The Ethiopian defense force cyber-unit, which was established in 2018 to combat the emerging threat of cyber war after the political and security-sector reform (Xinhua. 2018;Yirga,2022).

2.4.3.5 Cyber security Policy Framework in Ethiopia

THE NATIONAL ICT POLICY AND STRATEGY 2009

The Ethiopian government has implemented a comprehensive ICT policy and strategy that includes considerations for cybersecurity. This policy acknowledges the importance of protecting the national electric communications system, which encompasses both institutional and

individual security. Additionally, it aims to enhance public trust and safeguard the integrity of data and networks. Furthermore, the policy seeks to combat cybercrime and ICT misuse, which contributes to the fight against national, regional, and international crimes such as fraud, organized crime, and terrorism. It also addresses the national security implications that arise from the widespread use of ICT in the economy and society. Lastly, the policy aims to build the capacity of government agencies responsible for implementing and monitoring the ICT policy, as well as preventing and controlling cybercrime (Halefom, 2015).

The National Information Security Policy of 2011

The National Information Security Policy of 2011 is the first cybersecurity policy in Ethiopia; the policy addresses that the country is vulnerable to cybercrimes and the need for minimizing threats and vulnerabilities the policy also addresses ICT with cybersecurity implication in regards to the legal system and security strategy. (as cited in Halefom, 2015: 11). The policy is adopted to address the challenges related to the increasing dependability on information technology and it emphasized protecting the country information assets, national security, individual privacy from organized criminals, cyber terrorism, political extremists and state sponsored cybersecurity threats. Furthermore, the policy is "an integral part of the national security policies and strategies and other operational activities of the country and it consider It sees information security as a systematic security framework including the political economical social legal technical and administrative dimension. That Developed in a holistic approach." (Abenzer, 2019: 25).

2.4.4 Related Works

Existing literature on cybersecurity in Ethiopia has mainly focused on the legal and technical aspects of cybercrime, such as legal measures, strategies, and policies to combat it (Halefom, 2015; Kinfe,2016; Misgana,2016; Abenezer,2019). However, there is a significant research gap regarding cybersecurity in the context of national security, particularly in Ethiopia. In this section, four pieces of literature that focus on the state of cybersecurity in Ethiopia are reviewed.

The first literature reviewed is an article by Halefom (2015) titled "The State of Cyber Crime Governance in Ethiopia," which critically assesses the Ethiopian government's strategies to combat cybercrime across the dimensions of cyber security policies, legal frameworks, and institutional structures. Halefom employs empirical analysis and policy evaluation to advocate

for enhanced measures aimed at bolstering Ethiopia's cyber resilience and security infrastructure. He highlights the rapid expansion of internet connectivity in Ethiopia as transformative but also exposes vulnerabilities to cyber threats, particularly with the increased adoption of mobile technologies and financial services such as mobile money and ATMs (Halefom, 2015, p. 7).

Central to Halefom's findings is the identification of deficiencies within Ethiopia's cybersecurity governance framework. He identifies gaps in policy formulation and implementation across various sectors, emphasizing the absence of robust procedural frameworks within organizations to effectively manage cyber incidents. Halefom also highlights a prevalent culture of underreporting cybercrime, driven by public distrust in law enforcement effectiveness and concerns about potential negative consequences (Halefom, 2015, p. 2).

Despite these insights, Halefom's study reveals notable research gaps that require further investigation. Specifically, it overlooks the evolving landscape of state-sponsored cyber threats, which are increasingly significant on a global scale. Moreover, the study does not adequately consider the socio-economic, political, and technological factors that contribute to Ethiopia's cybersecurity challenges (Halefom, 2015).

Furthermore, the study's methodology is constrained by its reliance solely on a survey questionnaire, which may not comprehensively capture the intricate and dynamic nature of cybercrime. Additionally, while the study identifies the escalating risks of cybercrime, it lacks concrete case studies or specific examples to illustrate these threats effectively. Moreover, Halefom's recommendations primarily focus on proposed actions without delving into the practical aspects of how to implement a cybersecurity governance framework or model (Kibreab, 2020, p. 6).

To address these gaps, a new study could deepen the analysis of state-sponsored cyber threats and their implications for national security within Ethiopia. Methodologically, integrating diverse research methodologies such as case studies and expert interviews would enrich the understanding of cybersecurity dynamics and enhance the applicability of research findings.

The second empirical research under review is the master's thesis by Abenezer (2019) titled "Developing National Cyber Security Strategy for Ethiopia." This study emphasizes the urgent need for a national cybersecurity strategy to address escalating cybersecurity threats at the national level. It advocates for Ethiopia to learn from the experiences of other countries and international guidelines to formulate a flexible and dynamic national cybersecurity strategy. The

study argues that the absence of such a strategy in Ethiopia leaves a significant gap in combating cybersecurity threats effectively. It highlights Ethiopia's strategic position as the African Union's headquarters and its potential to become a digital transformation hub in the region, underscoring the necessity for a robust national cybersecurity framework.

Abenezer (2019) suggests that creating and implementing a national cybersecurity strategy is a critical step towards enhancing Ethiopia's cybersecurity landscape. However, he emphasizes that the strategy should align with the country's political, operational, financial, and technological contexts (Abenezer, 2019, p. 13). The thesis provides recommendations for Ethiopia's national cybersecurity strategy based on an analysis of local information and communication technology, expert opinions, best practices from other countries, and international guidelines that resonate with Ethiopia's strategic goals and priorities.

The study points out that Ethiopia's existing information security policy is outdated, especially given the country's ongoing economic reforms and critical projects. This necessitates the development of a comprehensive national cybersecurity strategy that reflects Ethiopia's overall strategic objectives and priorities (Abenezer, 2019, p. 13).

However, the research has notable gaps. It suffers from limited access to critical data, an insufficient sample size for drawing conclusive insights on cybersecurity challenges in Ethiopia, a lack of statistical analysis on cybersecurity incidents, and an overreliance on qualitative data. Additionally, the study does not adequately consider the unique contextual aspects of Ethiopia's cybersecurity landscape and relies heavily on the experiences of other countries without fully integrating local sociopolitical dynamics.

To address these gaps, the new study plans to incorporate a diverse panel of experts knowledgeable in Ethiopian cyber and national security. It aims to integrate practical evidence and case studies across various dimensions of cybersecurity and national security. By examining sociopolitical factors, local political intricacies, and geopolitical dynamics, the research seeks to provide a more holistic analysis. Furthermore, the study intends to explore broader economic, social, and political influences on cybersecurity threats.

The third literature reviewed is the master's thesis conducted by Tewodros Getaneh in June 2018, titled "Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia: Towards Tailoring the Cyber Security Framework." This study utilized a mixed-methods approach to investigate cybersecurity challenges within three essential infrastructures in

Ethiopia: Ethiopian Electric Power, Ethiopian Electric Utility, and Ethiopian Telecom. Grounded in the pillars of Legal, Technical, and Capability Building outlined by the International Telecommunication Union (ITU), the study revealed a concerning increase in cybersecurity threats across these infrastructures. It highlighted vulnerabilities to cyberattacks, including nation-state assaults, email attacks, hacktivist threats, web-based attacks, criminal activities, and insider threats. Additionally, the research underscored various obstacles faced by these critical infrastructures, such as a lack of in-house expertise, challenges in identifying security alerts, limited technological support, and inadequate security protocols (Tewodros, 2018).

However, the study exhibited significant gaps. It focused solely on three critical infrastructures, omitting crucial data from organizations like the Information Network Security Administration (INSA). The absence of independent verification and real-world examples of cybersecurity incidents undermined the study's reliability. Furthermore, the analysis did not consider political, social, and economic influences, and there was an unclear rationale for selecting specific infrastructures.

To address these deficiencies, the new study introduces a novel approach involving a diverse group of cybersecurity and national security experts to enhance the research's credibility and relevance. By broadening data collection to include inputs from institutions like INSA and implementing independent validation processes with empirical evidence from reputable sources, the study aims to provide a more comprehensive understanding of Ethiopia's cybersecurity landscape. Furthermore, the incorporation of practical cybersecurity incident examples, analysis of broader contextual factors, and transparent rationale for infrastructure selection will elevate the study's methodological robustness. These enhancements are designed to fill the identified research gaps and offer a holistic perspective on cybersecurity practices and challenges in Ethiopia.

The last empirical research preferred for the review is the article that was studied by Yirga Badma in 2022 with the title "ሳይበር ደህንነት በኢትዮጵያ እና ለብሔራዊ ደህንነት ያለው አንድምታ (Cybersecurity In Ethiopia and Its Implication for National Security)." The purpose of the study was to analyze the current state of cyber security in Ethiopia, identify best practices in cyber security, and propose recommendations for policies for reducing the impact of cyber security on national security. The researcher used a mixed-methods research approach and gathered the necessary data from questionnaires, interviews, and archived data from four Ethiopian

government institutions with national security as well as cyber security missions, namely the Ethiopian Defense Force, the Information Network Security Administration, the Financial Security Information Center, and the Ministry of Foreign Affairs.

According to the study, while cybersecurity threats might seem minimal in Ethiopia, they have been rising steadily in the past decade, posing a significant threat to Ethiopia's national security. As stated by the researcher, the ongoing involvement of multiple countries in cyber operations has resulted in a significant increase in high-risk cyber incidents. Based on the study, although efforts are being made to mitigate the impact of these cybersecurity threats, they are unlikely to be sufficient or effective in light of the level of the threat. The researcher further stated that there are limitations in national and institutional cyber security policy and strategy, legal framework, organization, capacity building, coordination, and cooperation efforts to combat the rising cybersecurity threats. Moreover, the researcher noted that cybersecurity has a significant effect on national security, which implies that it disrupts the normal functioning of a country's national security apparatus (diplomatic, informational, military, economic, etc.). As a result, significant steps need to be taken at the national and institutional levels to mitigate the risk of cybersecurity threats to national security by maintaining a strong cybersecurity posture.

The researcher also suggested that, in terms of organization, it is crucial to develop a National Cyber Security Council consisting of cyber security institutions that will concentrate primarily on national cyber matters. This institution can be held responsible by the National Security Council, and it may formulate its strategy and take measures to boost the efficiency of its current operations at the national and institutional levels.

However, the research has notable gaps. The study primarily relied on data from government institutions, overlooking the insights that could be gained from the private sector and non-governmental organizations. This limitation hinders a holistic view of the cybersecurity landscape in Ethiopia.

Furthermore, while the researcher suggested the establishment of a National Cyber Security Council akin to those in other countries, there is a lack of comparative analysis with existing practices in other nations, and the practical implementation of such a council in the Ethiopian context remains unclear. This gap raises questions about the feasibility and effectiveness of adopting similar structures in Ethiopia without contextualizing them within the country's unique cybersecurity challenges and institutional frameworks.

Moreover, the study extensively discussed the increasing cybersecurity threats facing Ethiopia and their implications for national security but lacked concrete examples or cases to illustrate the severity of these threats. Without tangible instances to demonstrate the real-world impact of cybersecurity incidents, the study's analysis may lack the necessary depth and specificity required to understand the actual risks faced by Ethiopian critical infrastructures and national security apparatus.

To address these gaps, the new research tried to involve private cybersecurity experts alongside government institutions to provide a more comprehensive perspective on cybersecurity challenges in Ethiopia. By incorporating insights from the private sector and non-governmental organizations, the study aims to enrich its analysis and offer a more nuanced understanding of the cybersecurity landscape in the country.Furthermore, the new research will emphasize the inclusion of concrete examples and case studies to illustrate the impact of cybersecurity threats on Ethiopian national security. By showcasing real-life incidents and their implications, the study aims to provide a more compelling narrative of the risks faced by the country and underscore the urgency of strengthening cybersecurity measures at both national and institutional levels.

Chapter Three

Research Methodology

3.1 Introduction

This chapter discusses the philosophical assumptions of the study, the research approach and design, sampling techniques, sample size, data types, data collection procedures and techniques, data analysis methods, and ethical considerations.

3.2 Philosophical assumption

Based on the research objectives, this study employed a pragmatic philosophical approach. Pragmatism is not restricted to any particular philosophy or worldview. The pragmatism emphasis is on the outcomes of research, the primary significance of the question presented rather than the methodologies, and the application of different data-gathering techniques to better understand the problems under study. As a consequence, it is pluralistic and focused on "what works" and practical application (Creswell & Plano Clark, 2018). Thus, pragmatism is particularly well adapted for complex, dynamic, and rapidly evolving challenges, such as cyber security and national security, which demands multiple perspectives and methodologies to properly understand the problem.

In regards to ontological beliefs, the researcher believes that reality exists; nevertheless, in the context of cybersecurity, it is dynamic and constantly evolving as a result of multiple technological and sociopolitical variables. Furthermore, the escalation of cybersecurity threats in Ethiopia is considered to be the result of a complex interplay of several different factors (technological, economic, sociopolitical, etc.). To understand the complex contributing factors, various perspectives and methods are required. Moreover, to view the multifaceted aspects of national security that are affected by the emerging threat of cyberspace, multiple theoretical and methodological approaches are very important.

Table .3. 1 : Justification of Pragmatism

Philosophical Assumption	**Description**	**Justification**
Ontological	Reality in cybersecurity is dynamic, shaped by multiple technological and sociopolitical factors.	Reflects the evolving nature of cybersecurity threats and their complex impact on national security.
Epistemological	Knowledge is derived from diverse perspectives and methods to grasp the complexity of contributing factors.	Ensures a thorough understanding of the multifaceted cybersecurity landscape and its national security implications.

3.3 Research Approach

Based on the research objectives, this study used a mixed-methods approach. The mixed methods approach involves the collection of quantitative and qualitative data and integrating or combining them to obtain insights or inferences (Creswell, 2013). Both quantitative and qualitative research approaches were integrated to gain a better understanding of cyber security threats and their implications for Ethiopia's national security. The frequency and classification of cybersecurity threats primarily depend on quantitative data; however, the intensity and risk resulting from these threats must be evaluated using both qualitative and quantitative analyses. Furthermore, some of the factors that contribute to these threats are easily quantifiable (such as economic and technological elements), whereas others, such as political and social factors, are profoundly contextual and require in-depth qualitative analysis. Moreover, the implications of cybersecurity threats on national security can be quantitatively measured from economic and technological aspects; however, their impact on social, cultural, psychological, and political aspects requires an in-depth qualitative analysis. Generally, to examine the complicated dynamics of cybersecurity and the resulting implications for Ethiopian national security, using both quantitative and qualitative research approaches is mandatory.

3.4 Research Design

The design preferred in this study was an explanatory sequential mixed-method design. According to Creswell and Clark (2018), explanatory sequential design explains initial

quantitative findings using qualitative data by integrating the two databases. This two-phase design begins with collecting quantitative data and analyzing the findings, and in the subsequent phase, collecting and analyzing qualitative data to further explain the results from the quantitative analysis. In this design, the fundamental idea is that qualitative data gathering and analysis depend directly on the results of quantitative data. In this study, the research process started with the collection of quantitative data regarding cybersecurity incidents in Ethiopia over the past decade. In the second phase, qualitative data were collected and analyzed for further explanation and in-depth analysis of these cyber incidents, the factors behind them and their implications for national security. Moreover, in this study, qualitative data were used to provide further explanation, corroboration, and triangulation of the data obtained from the quantitative results.

3.5 Sample Size and Techniques

The research was primarily done based on data from two government institutions (INSA and the Ethiopian Defense Force), and purposive sampling was used for selecting study participants with expertise in the two government institutions, with a particular emphasis on cyber security as well as national security. The sample technique was chosen purposefully due to the relatively small number of cybersecurity professionals, making sure that the participants chosen could provide reliable information on the present state of cybersecurity in Ethiopia and its implications for national security. As a result, the requirements for selection revolved around knowledge, responsibility, and specialization in cybersecurity and national security in the Ethiopian context.

The study included 84 cybersecurity officers, including 42 from INSA and 28 from the Ministry of Defense (particularly from the Ethiopian Defense Force's Cyber Directorate, the Ethiopian Air Force's Cyber Directorate, and the Defense Engineering College). To make the study more inclusive, the researcher tried to find cybersecurity experts from the private sector; however, the researcher was only able to find 14 cybersecurity experts from the private sector, particularly from the banking industry. As a result, all 14 experts participated in the study. Regarding the open interviews, 16 senior cybersecurity officers were purposely selected from the closed-ended survey questionnaire participants to provide further clarification and explanation of the quantitative data gathered from the previous survey.

Table 3. 2 . Purposive Sampling

Institutions	Sample Size (Closed-ended Survey)	Sample Size (Open Interview)	**Sample Type**
INSA	42	7	Purposive
Ethiopian Defense Force	28	4	Purposive
Private Sector (Banking)	14	3	Purposive
Total	84	14	

3.6 Source of Data

This study used data from both the primary and secondary sources. The primary data sources were a closed-ended questionnaire distributed to cybersecurity experts, and an open-ended interview with selected experts. Secondary data were sourced from INSA's reports on cybersecurity incidents, media outlets, press releases, annual reports, Internet platforms, websites, and social media channels. These sources are critical to achieving the research objectives.

3.7 Data Collection Instruments

The study's data-collection instruments included document reviews, questionnaires, open interviews, and case studies. Document reviews were used to gather statistical records of cybersecurity threat incidents, a questionnaire to collect quantitative data from cybersecurity officers to generalize the findings, and an open interview and case study to obtain information that could provide further clarification and explanation to the areas that required clarification.

3.7.1 Document Analysis

Annual incident reports from INSA have been utilized to review the state of cybersecurity in Ethiopia throughout the past decade. These incident reports are important to understand the evolution of cybersecurity threats over the past few years.

3.7.2 Questionnaire

Primary quantitative data for the study were gathered via a closed-ended questionnaire and distributed to 84 participants. The questions for the survey were selected following an intense

literature assessment and observations and organized into four parts, following the research objectives. The initial part of the questionnaire included the demographic variables of the participants, including their academic status, work experience, and specialized certification in cybersecurity. The second part of the questionnaire included Ethiopia's cybersecurity threats over the past few decades (based on statistical reports). The second section focuses on the factors that contribute to cybersecurity threats in Ethiopia, and the last section discusses how the rise in cybersecurity threats affects Ethiopian national security. The questionnaire response format utilized a five-point Likert scale that ranged from "strongly disagree" to "strongly agree," with from one to five coded options (one for strongly disagree and five for strongly agree).

3.7.3 Key Informant Interview

An open interview was conducted to select participants for the questionnaire. Open interview questions were selected from the quantitative results for further explanation and clarification of concepts that could not be addressed merely by quantitative data. All the open interviews were conducted in Amharic.

3.7.4 Case Studies

Selected cybersecurity threat incident cases were provided to solidify the results obtained from the quantitative and qualitative data-collection instruments. Case studies are important for providing real-world insights that complement the broader insights that complement the state of cybersecurity threats, the factors behind these threats, and their implications for national security.

3.8 Data Collection Procedures

This study employed various data-gathering methods and procedures to obtain comprehensive data on the state of cybersecurity in Ethiopia and its implications for national security. Based on the explanatory sequential design guidelines, a quantitative data collection process was carried out in the first phase. As a result, statistical data on cybersecurity threats in Ethiopia over the last ten years was collected from INSA. After analyzing the statistical reports, a closed-ended questionnaire was provided to all survey participants to collect further data on the cybersecurity threat reports, the factors behind these threats, and their impact on national security. After collecting and analyzing the quantitative data, qualitative data is collected by using an open interview with the previous survey participants to further clarify and explain the quantitative

data. Last but not least, some case studies are included to further solidify the previously collected data.

3.9. Data Analysis Methods and Procedures

Both quantitative and qualitative data were gathered and analyzed separately in the sequence based on the mixed-method explanatory sequential design guidelines.

3. 9 .1 Quantitative Data Analysis

Before data analysis, the data were cleaned to confirm that they were completed correctly. Quantitative data analysis was performed using SPSS version 27 to investigate the frequency distribution. Furthermore, the weighted mean was utilized to provide a more complete analysis by assigning numerical values to each response option. Percentages were used to indicate how the variables were distributed in relation to the overall sample size. To visually show the distribution of the variables, bar graphs and tables were used.

3. 9 .2 Qualitative Data Analysis

The interview recordings were transcribed and cross-checked for errors verbatim, and the Amharic data were then translated into English. The findings were analyzed using Braun and Clark's (2006) six-phase thematic analysis guidelines, which include: (1) becoming familiar with the data, (2) generating preliminary codes, (3) identifying themes, (4) examining themes, (5) defining themes, and (6) writing. The results were presented systematically, including both predefined and emerging themes.

3.10. Ethical Considerations

This study presents various ethical issues that researchers should evaluate and anticipate. First, the researcher submitted an official letter to the selected institutions, seeking permission to conduct surveys and interviews, in addition to accessing pertinent papers that may serve as primary sources. The researcher asked neutral questions during the interviews to avoid offending or insulting the individual or the institution. Furthermore, the researcher endeavored to assess the data objectively, free of bias or connection to a specific viewpoint or ideology. The researcher also attempted to report the findings as precisely as possible with no deceptive changes.

CHAPTER FOUR
DATA PRESNTATION

This chapter presents and analyzes the study results in three main parts based on the research objectives. Firstly, it discusses Cybersecurity Threat Incidents in Ethiopia over the Past Decade . Secondly, it explores the factors contributing to the escalation of cyber security threats and how these threats affect Ethiopian national security. Additionally, towards the end of the chapter, specific cases of cyber security threats are presented to solidify the results.

4.1 Cybersecurity Threat Incidents in Ethiopia over the Past Decade

To analyze the cyber-security threats that have occurred in Ethiopia over the past ten years, statistical data was gathered from the Information and Networking Security Administration (INSA). The following table presents the data reflects the number of reported cyber-attacks in Ethiopia from 2012 to 2023.

Table 4. 1 Cybersecurity Threat Incidents in Ethiopia for the Past Decade

Year	**Cyber Attacks**	**Percentage Increment**	**Escalation**	**Total Escalation**	**General increment in Percentage**
2012/13	59	-	-	-	-
2013/14	65	10.17%	6	6	10.17%
2014/15	51	-21.54%	-14	-8	-13.56%
2015/16	214	319.61%	163	155	264.41%
2016/17	479	123.83%	265	420	611.86%
2017/18	576	20.25%	97	517	776.27%
2018/19	791	37.33%	215	732	1140.68%
2019/20	1075	35.90%	284	1016	1622.03%
2020/21	2898	169.58%	1823	2839	4711.86%
2021/22	8845	205.04%	5947	8786	14875.42%
2022/23	9689	9.54%	844	9630	**16322.03%**

Source: Information collected from the Ethiopian Information Network Security Agency (INSA).

The analysis of cybersecurity threat incidents in Ethiopia over the past decade reveals a concerning trend of a significant rise in cyber-attacks. Data from the Information and Networking Security

Administration (INSA) shows a dramatic increase in reported incidents, from 59 in 2012/13 to 9689 in 2022/23, indicating a clear upward trajectory. Notable spikes were observed in 2015/16 and 2020/21, with a particularly steep increase of 205.04% between 2020/21 and 2021/22, resulting in a substantial escalation of 5947 attacks during this period. By 2022/23, the cumulative growth amounted to an alarming increase of 9630 attacks, representing an overall increment of 16322.03%.

However, discrepancies arise when comparing these findings with external sources. Kaspersky reported a higher number of attacks, with 18000 attacks and 30000 ransomware incidents in Ethiopia in 2023 alone, contrasting with lower figures from local sources. Business Insider Africa also identified Ethiopia as the third African country with the highest cybersecurity threats, contradicting local reports that downplayed the severity of these threats.

Survey responses from cybersecurity experts further support the notion of an escalating cybersecurity threat landscape in Ethiopia. A vast majority of experts acknowledged a significant increase in threats over the past decade. The survey results indicate that 87.8% of participants believe that cybersecurity threats in Ethiopia have increased, while only 1.5% noted a decrease and 3.7% stated that the threat level remained the same. The weighted mean of 4.45 suggests that the average response falls between the "highly increased" and "extremely increased" categories, emphasizing the consensus among experts regarding the heightened cybersecurity risks in the country.

Table 4.2 Cyber-Security Threats over the Past Decade: survey response

Response	N	%	Numerical Value
Decreased	1	1.5%	1
Remained the same	3	3.7%	2
Moderately Increased	6	7.3%	3

Response	N	%	Numerical Value
Highly increased	20	24.4%	4
Extremely increased	52	63.4%	5
Weighted Mean			4.45

The quantitative results from INSA data and closed-ended survey results are further clarified and explained by cybersecurity experts through open interviews. These experts consistently stated an exponential increase in cybersecurity threats in Ethiopia over the past decade, articulating the massive escalation of these threats in various ways but with a consistent underlying idea. This analysis categorizes the interview responses into three primary themes, providing a comprehensive understanding of the trends of cybersecurity threats in Ethiopia.

Theme 1: Frequency and Intensity of Cybersecurity Threats

The findings show that all participants explained that cybersecurity threats in Ethiopia over the past decade have escalated significantly, not only in terms of frequency but also in intensity. They articulate the exponential escalation of the threats in various ways, but with a consistent underlying idea. A senior cybersecurity officer from INSA described the frequency and intensity of the threat:"Apart from the frequency, there has been a significant increase in the intensity of high-risk cybersecurity threats. The intensity of the threats may be difficult to analyze quantitatively, but their economic, social, and political effects are plainly visible."Moreover, a senior cybersecurity officer from the Ethiopian Defence Force discussed the recent sophistication of cybersecurity threats:

> *Cybersecurity threats are becoming more sophisticated, unpredictable, and undetectable over time. Recently, highly volatile and undetectable cyber-attacks have increased. This involves advanced persistent threats (APTs), which are*

persistent and strategic cyber assaults designed to persist undetected for a prolonged period that could result in critical damage to various infrastructures.

A senior cybersecurity officer from INSA also described the escalation of high-risk cybersecurity threats, particularly in relation to state-sponsored cyber-attacks. He noted:"State-sponsored cyber-attacks are on the rise at higher rates. Such cyber-attacks are highly risky, as their main targets are against critical infrastructure and sensitive government data."According to the respondents, the intensity of cybersecurity threats is measured through their economic, social, and political impacts, as well as their technical sophistication. While quantitative analysis may be challenging, the qualitative effects are evident. Economic disruptions, social instability, and political ramifications are clear indicators of the heightened intensity of cyber-attacks. The escalation is further demonstrated by the increasing frequency of advanced persistent threats and state-sponsored attacks targeting critical infrastructure. These high-risk threats underscore the evolving and growing cybersecurity challenges in Ethiopia.

Theme 2: Cybersecurity Threats vs. Digitalization

The theme delves into the relationship between cybersecurity threats and the pace of digitalization in Ethiopia, highlighting the disparity between the two.A Senior Cybersecurity Officer from INSA stated, "Cybersecurity threats are increasing worldwide due to reliance on digital technology, and Ethiopia is facing more threats than expected." This sentiment was echoed by a Senior Cybersecurity Officer from the Ethiopian Airforce, who emphasized that the rate of cyber threats in Ethiopia is outpacing the country's digital progress.Another Senior Cybersecurity Officer from INSA also pointed out,

> In the context of Ethiopia, despite advancements in digital transformation and internet accessibility, these developments are occurring at a slower rate compared to economic growth and similar developing countries. This lag in digitalization relative to economic expansion is notable. However, cybersecurity threats are escalating at a rapid pace, surpassing the growth of internet penetration and overall digital technologies.

This theme underscores the critical need to align cybersecurity measures with the rapidly evolving digital landscape in Ethiopia. As the country moves towards greater digital integration, addressing the widening gap between cybersecurity readiness and digitalization becomes imperative to safeguard critical infrastructure and sensitive data from escalating threats.

Theme 3: underreported Cybersecurity Incidents

In relation to the yearly incident reports on cybersecurity, some participants indicated that there could be instances of underreported significant cyberattacks. A cybersecurity officer from Oromia Bank highlighted the potential for substantial underreporting of such cybersecurity threat incidents. He mentioned:

> *Cybersecurity threats in Ethiopia could be more pervasive than what is officially declared. Factors behind this underreporting might include organizations' hesitance in disclosing incidents out of fear of losing their reputation, a surge in stealthy cyber assaults that remained undetected for a long time, and a lack of awareness regarding the advantages of reporting such incidents. Accordingly, the real magnitude of cybersecurity incidents in Ethiopia is possibly far larger and considerably more extensive than the official statistical reports.*

Overall, the analysis underscores the need for increased transparency and proactive reporting mechanisms within Ethiopia's cybersecurity landscape. Addressing barriers to reporting and enhancing awareness about the implications of underreporting are essential steps towards gaining a more comprehensive understanding of cyber threats in the country. Bridging the gap between official reports and the actual incidence of cyberattacks is crucial for developing effective mitigation strategies and strengthening overall cybersecurity resilience in Ethiopia

4.2 Factors Contributing to the Rise of Cybersecurity Threats in Ethiopia

While various factors play a role in the increase of cybersecurity threats worldwide and in the region, this study specifically examines the factors influencing cybersecurity threats in Ethiopia. Through an in-depth review of literature, media reports, and firsthand observations, four primary factors were identified. To evaluate the impact of these factors on cybersecurity threats, a survey was conducted using closed-ended questionnaires and open interviews, with the data analyzed using descriptive statistics and thematic analysis. The subsequent sections will present and analyze the findings obtained from this study.

Table 4.3: Survey Results: Factors Behind Ethiopian Cybersecurity Threats

Factors	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree	Weighted Mean
Rapid Technological Adoption Without Sufficient Cybersecurity Infrastructure	2.4%	4.9%	12.2%	57.3%	23.2%	3.97
Outdated Cybersecurity Policies And Legal Frameworks	1.2%	7.3%	7.3%	54.9%	29.3%	4.06
Local Political Tensions	3.7%	4.9%	14.6%	54.9%	22.0%	3.91
Geo-Political Tensions	2.4%	3.7%	12.2%	61.0%	20.7%	3.97

1. **Rapid Technological Adoption Without Sufficient Cybersecurity Infrastructure**:

The analysis of rapid technological adoption without sufficient cybersecurity infrastructure in Ethiopia reveals a high level of agreement (80.5%) among participants regarding its significant contribution to escalating cybersecurity threats. This widespread recognition highlights the correlation between rapid technology adoption and inadequate cybersecurity measures. The weighted mean of 3.97 further emphasizes this perception as a key driver of cybersecurity threats. Additionally, only 7.3% of respondents disagreed, indicating a strong consensus on the associated risks.

To gain deeper insights, open interviews were conducted, identifying several key themes. One prominent theme is rapid technological adoption without sufficient cybersecurity infrastructure. A senior officer from the Information Network Security Agency (INSA) stated:

> *Ethiopia's swift technological advancement, particularly in digitalization and the Internet of Things (IoT), has resulted in several benefits and improved functionalities. However, the lack of sufficient cybersecurity infrastructure has made organizations and critical sectors vulnerable to cybersecurity threats. Counting on digital technology, in the absence of strong cybersecurity*

infrastructure and measures, has facilitated a fertile environment for cyber offenders to exploit vulnerabilities. This gap is mostly noticeable in Africa, particularly in Ethiopia, where the adoption of digital technology is increasing but the protective measures are lagging.

Furthermore, another theme identified was foreign technology dependency. Participants explained that relying on foreign technology, especially for security purposes, increases Ethiopia's vulnerability to cybersecurity threats. Another senior officer noted, "Foreign technology dependency, particularly on security technologies, has made developing countries like Ethiopia more vulnerable to cybersecurity threats." An officer from the Ethiopian Defense University also described the situation: "The country's dependency on foreign technology has made it more vulnerable to cybersecurity threats. Consequently, there has been a noticeable surge in initiatives by the Ethiopian government to nurture indigenous security technologies as a strategic measure to address this vulnerability."

Overall, the analysis underscores the need for Ethiopia to align technological advancement with robust cybersecurity infrastructure and reduce dependency on foreign technologies to effectively mitigate cybersecurity threats and protect critical sectors from escalating risks.

2. **Outdated Cybersecurity Policies And Legal Frameworks**:

According to the results, most participants (84.2%, combining 54.9% who strongly agree and 29.3% who agree) believe that outdated cybersecurity policies and legal frameworks contribute to the rise of cybersecurity threats in Ethiopia. The weighted mean of 4.06, the highest value relative to other factors mentioned, suggests that respondents firmly believe this factor significantly escalates the threats. Conversely, only a small percentage (8.5%, combining 1.2% who strongly disagree and 7.3% who disagree) did not support this statement, indicating that only a few participants do not consider outdated policies and frameworks as major contributors to cybersecurity threats.

To gain deeper insights, open interviews were conducted, revealing key themes. One primary theme is the impact of obsolete cybersecurity policies and strategies. A senior cybersecurity officer from INSA mentioned,

Contemporary cybersecurity challenges are evolving rapidly and becoming volatile; therefore, policies and strategies that take these new challenges into

account are urgently needed. The lack of regular updates of policies and strategies has increased susceptibility to cyber threats by allowing cyber offenders to exploit vulnerabilities in the existing framework.

Similarly, a seasoned cybersecurity officer from the Ethiopian Defense Force Cyber Directorate pointed out that outdated cybersecurity policies and strategies, when compared with recent digital initiatives and reforms, have exacerbated vulnerabilities. He stated:

> Obsolete cybersecurity strategies and policies have contributed to cybersecurity vulnerabilities in Ethiopia. With rapid digitalization, particularly following initiatives such as the Ethiopian 2025 Digital Strategy, which has introduced new digital technologies and platforms, existing cybersecurity policies and strategies have not been adapted to these emerging technological reforms. Consequently, they may not adequately address critical security concerns with emerging technologies.

Participants also noted that cybersecurity issues are closely connected to global and regional affairs. However, current Ethiopian policies and strategies do not align well with the dynamics of the global cyber context. One cybersecurity officer from Awash Bank emphasized, "As cybersecurity is a cross-border and global issue, the associated policies should be revisited, considering international and regional developments. I think the Ethiopian National Cybersecurity Draft Policy that has been recently prepared is in line with international and regional cyberspace trends."

Overall, the analysis underscores the urgent need for Ethiopia to regularly update its cybersecurity policies and legal frameworks to reflect contemporary challenges and align with global and regional developments. By doing so, Ethiopia can more effectively mitigate cybersecurity threats and protect its critical sectors from escalating risks.

3. **Local Political Dynamics**:

According to the survey findings, a significant majority of participants (22.0% strongly agree and 54.9% agree) believe that "local political dynamics" contribute to the rise of cybersecurity threats in Ethiopia. The weighted mean of 3.91 further clarifies that participants tend to agree on the impact of local political dynamics on increasing cybersecurity threats. Conversely, only 8.6% of respondents (3.7% strongly disagreed and 4.9% disagreed) did not support this state

To gain deeper insights, open interviews were conducted, revealing several key themes. One prominent theme is the direct influence of Ethiopias domestic political dynamics on the escalation of cybersecurity threats. A senior cybersecurity officer from INSA stated,

> *Recently, it has become apparent that local political dynamics and the escalation of cybersecurity threats are directly proportional. When political tensions and conflicts are high, cybersecurity threats tend to increase in frequency and intensity. For instance, during elections and law enforcement operations, there has been a noticeable escalation in cyberattacks. Furthermore, at the time of prominent local political events and conflicts, there has been an escalation in hacktivism activities intended to propagate misinformation by hacking media platforms and websites.*

Another theme identified is the role of political groups and external political entities in escalating cybersecurity threats. A cybersecurity officer from the Ethiopian Defense Force elaborated, "Nowadays, numerous political groups with varying objectives are increasingly using cyberattacks as a means to propel their political aims and interests, either on their own or in alliances with external actors. Consequently, politically motivated cybersecurity threats have escalated in the country."

These qualitative insights provide a deeper understanding of the quantitative data, highlighting how local political dynamics exacerbate cybersecurity threats in Ethiopia. During periods of political tension, such as elections and conflicts, there is a notable increase in the frequency and intensity of cyberattacks. Political groups, both domestic and supported by external entities, use cyberattacks to further their objectives, leading to a rise in politically motivated cybersecurity threats.

Overall, the analysis underscores the critical need for Ethiopia to address the intersection of political dynamics and cybersecurity. Developing robust cybersecurity strategies that can withstand the pressures of local political tensions and mitigate the influence of politically motivated cyberattacks is essential for protecting the nation's digital infrastructure and maintaining stability.

4. Geo-Political dynamics:

The analysis of geopolitical dynamics indicates a strong consensus among participants regarding its significant role in escalating cybersecurity threats in Ethiopia. A substantial majority (61.0% agree and 20.7% strongly agree) perceive geopolitical dynamics as contributing significantly to the

increase in cybersecurity risks, reflected in a weighted mean of 3.97. Conversely, a minority (2.4% strongly disagree and 3.7% disagree) holds the view that geopolitical dynamics do not augment cybersecurity threats.

Qualitative insights from open interviews further elucidate how recent geopolitical developments have heightened cybersecurity risks within Ethiopia. A senior cybersecurity officer from the Ethiopian Defense Force emphasized:

> *Nowadays, states and state-sponsored actors increasingly engage in cyberattacks to further their national interests. This trend escalates during geopolitical conflicts, such as those related to the Grand Ethiopian Renaissance Dam (GERD). We've observed a notable increase in cyberattacks during these periods, potentially orchestrated by downstream countries aiming to influence negotiations.*

Another perspective from INSA highlighted global geopolitical factors exacerbating cybersecurity threats. According to a cybersecurity officer, "The absence of international conventions regulating cyberspace allows countries to conduct cyber espionage and warfare against perceived adversaries. Ethiopia's strategic location in the Horn of Africa and its abundant cross-border resources heighten its susceptibility to various high-risk cyberattacks."

Additionally, a senior cybersecurity officer from INSA noted, "External interventions in Ethiopia's internal affairs have significantly escalated cybersecurity threats, likely perpetrated by various states and state-sponsored cyber actors."

These qualitative findings complement the quantitative data, illustrating how geopolitical dynamics directly contribute to escalating cybersecurity threats in Ethiopia. During times of heightened geopolitical tensions, such as those around the GERD negotiations, cyber incidents aimed at influencing political outcomes intensify. Ethiopia's strategic positioning and regional significance in the Horn of Africa amplify its vulnerability to cyber espionage and offensive cyber operations from external actors seeking to exploit geopolitical rivalries.

4.3 The Impact of Cybersecurity Threats on Ethiopian National Security

To assess the cybersecurity threat and its implications for the national security of Ethiopia, five Linkert scale questions were asked to cybersecurity officials and experts. In this section, the results of this survey questionnaire will be presented and analyzed using basic descriptive statistics such as percentage, frequency, and weighted means.

In exploring the impact of cybersecurity threats on Ethiopian national security, both quantitative survey results and qualitative insights from open interviews provide a comprehensive understanding. Survey findings reveal that 84.2% of participants recognize these threats as influential to national security, supported by a weighted mean of 4.015, indicating broad consensus on their severity. However, a minority, comprising 7.3% of respondents, maintained a neutral stance, while 8.6% disagreed with this viewpoint.

Table 4. 4 Survey Responses Cybersecurity Threats Impact Ethiopian National Security

Options	N	%	Numerical values
Strongly disagree	2	3.7%	1
Disagree	4	4.9%	2
Neutral	5	7.3%	3
Agree	37	53.7%	4
Strongly Agree	20	30.5%	5
Weighted mean			4.015

Qualitative interviews further enrich these findings by delving into expert perspectives. Across interviews, there was a consistent emphasis on the significant implications of cybersecurity threats for Ethiopian national security. Respondents highlighted the potential risks if preemptive measures are not adequately implemented. For instance, a senior cybersecurity officer from INSA emphasized, "While the threats have the potential to jeopardize national security, the current scenario does not indicate an imminent threat. However, if adequate security measures are not put in place and maintained, the consequences could threaten national security." This qualitative data not only reinforces the consensus on the seriousness of cybersecurity threats but also reveals varying viewpoints on their immediacy and underscores the necessity of proactive risk management strategies. Thus, the integration of survey data and qualitative insights presents a thorough analysis of how cybersecurity threats impact Ethiopian national security, underscoring the urgency for robust protective measures to safeguard national interests effectively.

Table **4. 5** How Cybersecurity Threats Impact Ethiopian National Security

Response Category	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree	Weighted Mean
By Affecting Sovereignty Through Nation-State Attacks	3.7%	3.7%	17.1%	45.1%	30.05%	3.94
By Causing Disruptions To Critical Infrastructures	3.7%	3.7%	7.3%	61.0%	24.4%	3.96
By Affecting The Political Dynamics.	1.2%	8.5%	12.2%	53.3%	24.4%	3.93

Impact on Sovereignty:

The findings from the closed-ended questionnaire reveal that 75.15% of participants (45.1% agree and 30.05% strongly agree) believe that cybersecurity threats undermine Ethiopian national security by affecting sovereignty through nation-state attacks. The weighted mean of 3.94 indicates a broad consensus among participants regarding this impact. Conversely, 17.1% of respondents were neutral, while 7.4% (3.7% strongly disagree and 3.7% disagree) did not support this viewpoint.

During the open interviews, participants provided deeper insights into how cybersecurity threats impact sovereignty. A cybersecurity officer from INSA highlighted the interference of foreign actors in Ethiopia's internal affairs through cyber warfare, stating, "Various foreign actors attempt to manipulate political and economic decisions in Ethiopia using cyber warfare, thereby violating our sovereignty and undermining the state's authority to manage internal matters independently."

Echoing this sentiment, a cybersecurity officer from the Ethiopian Air Force underscored the importance of securing cyberspace to safeguard sovereignty, saying, "In modern warfare, securing cyberspace is crucial for protecting sovereignty. Ethiopia recognizes cyberspace as a

military domain alongside land, airspace, and sea, making any cyber assault an attack on our sovereignty and national security."

Furthermore, another INSA cybersecurity officer likened these cyber threats to acts of invasion, remarking, "The digitalization of Ethiopia has exposed us to vulnerabilities exploited by foreign adversaries intent on undermining our sovereignty. Their ongoing attempts to invade our country through cyberspace pose a significant threat."

Additionally, concerns were raised about the impact of cybersecurity threats on law enforcement operations. A seasoned INSA cybersecurity officer highlighted these vulnerabilities, stating, "The security sector faces significant risks from cyber threats due to the widespread adoption of digital technology. Without adequate security measures, cyber operations could disrupt law enforcement, compromise sensitive information, and damage security infrastructure."

In conclusion, the analysis of both quantitative and qualitative data underscores the consensus that cybersecurity threats pose substantial risks to Ethiopian sovereignty. The open interviews enrich the understanding by highlighting real-world implications, including foreign interference, the militarization of cyberspace, and operational disruptions, thereby emphasizing the need for robust cybersecurity strategies to protect national sovereignty and security.

Critical Infrastructure Disruptions:

Based on the quantitative closed-ended survey questionnaire results, 84.4% of participants expressed that cybersecurity threats impact Ethiopian national security by disrupting critical infrastructure. Specifically, 61.0% agreed and 24.4% strongly agreed with this assertion, reflecting a weighted mean of 3.96, the highest recorded among responses. Conversely, 7.3% of respondents remained neutral, while 7.4% (3.7% strongly disagree and 3.7% disagree) did not support the statement.

In the open interviews, thematic analysis further elucidates the reasons behind this perception. Participants consistently highlighted the disruptive effects of cybersecurity threats on critical infrastructure in Ethiopia. A senior cybersecurity officer from INSA emphasized the economic repercussions, stating, "An effective cyber-attack on critical infrastructure would have a severe

negative impact on the overall national economy." This underscores the vulnerability of Ethiopia's limited financial and technological resources in recovering from such attacks.

Similarly, a senior cybersecurity officer from the Ethiopian Defence University pointed out broader economic implications, noting, "Cyber-attacks against financial and production sectors can disrupt trade, reduce production, and impact the economy." This observation underscores the interconnectedness of critical infrastructure with economic stability and national security.

Furthermore, a cybersecurity officer from Awash Bank highlighted governance challenges arising from such disruptions, stating, "Cyber-attacks on key infrastructure threaten the functionality of the government and erode public trust in its ability to secure critical services, potentially undermining its legitimacy." This perspective underscores the broader implications of cybersecurity threats beyond economic impacts.

Moreover, another INSA officer described critical infrastructure disruption as exacerbating existing challenges in security and economy, noting, "Cyber-attacks on critical infrastructure multiply other problems, posing threats to national security and stability."

Lastly, the seriousness of these threats was equated to acts of war by another officer, who argued, "Any cyber-attack on Ethiopia's critical infrastructure should be considered an act of war." This perspective underscores the strategic importance of cybersecurity defense in protecting national interests.

Impacts on Political Dynamics:

Based on the findings from the closed-ended survey questionnaire, 77.7% of participants (53.3% agree and 24.4% strongly agree) believe that cybersecurity threats impact the national security of Ethiopia by affecting political dynamics. A weighted mean of 3.93 further clarifies that participants tend to agree with this statement. Conversely, 12.2% of respondents were neutral, and 9.7% (1.2% strongly disagree and 8.5% disagree) did not support the view that cybersecurity threats affect political dynamics.

In the open interviews, participants elaborated on how cybersecurity threats influence national security by affecting local political dynamics. A cybersecurity officer from the Ethiopian Defence University highlighted hacktivism as a significant cybersecurity threat impacting local political dynamics in Ethiopia, stating:

In the Ethiopian context, hacktivism has emerged as a cybersecurity threat affecting local political dynamics. Both internal and external political groups with diverse agendas have targeted various media platforms and websites to disseminate misinformation that aligns with their political objectives. For instance, during the 2021 government inauguration, the official Facebook page of the Ethiopian Broadcasting Corporation was hacked to spread false information aimed at exacerbating political conflicts.

Echoing this sentiment, an officer from INSA emphasized how cyber threats disrupt political cohesion, stating:"Different political entities and hacktivists can significantly influence local political dynamics by compromising government social media platforms and websites. The dissemination of misleading information through these channels undermines societal solidarity and cohesion."Furthermore, another senior INSA officer detailed the multifaceted impact of cybersecurity threats on local political dynamics:

In Ethiopia, cybersecurity threats manifest in several ways that affect local political dynamics. First, attacks targeting critical infrastructure directly hamper government operations, exacerbating political unrest and local disputes. Second, foreign political entities leverage cyber warfare to intervene in local affairs, supporting specific armed groups and exacerbating existing conflicts. Third, cyber assaults on media outlets propagate misinformation that escalates ethnic tensions, particularly in ethnically diverse countries like Ethiopia.

In conclusion, the combined analysis of quantitative and qualitative data underscores the consensus that cybersecurity threats pose significant risks to Ethiopian national security by disrupting political dynamics. The qualitative insights from open interviews provide nuanced perspectives on how cyber threats, such as hacktivism and misinformation campaigns, undermine political stability and exacerbate existing tensions. This highlights the critical need for comprehensive cybersecurity strategies to protect political processes and national security in Ethiopia.

4.4 Cyber Security Threat Incidents in Ethiopia: Case Studies

This section presents case studies of cybersecurity threat incidents in Ethiopia sourced from government documents, media outlets, websites, interviews, and direct observation. The cases highlighted include cyberattacks against critical infrastructures and politically motivated cyberattacks (hacktivism) targeting Ethiopian government-owned websites and official social media pages.

4.4.1 Cyber-attacks against Ethiopian Critical Infrastructures

As reported by INSA, cyberattacks in Ethiopia primarily target critical infrastructures such as telecommunication centers, power grids, transportation systems, and security sectors. These infrastructures are crucial as their compromise could threaten national interests. This subsection outlines significant cybersecurity threat incidents against Ethiopian critical infrastructure.

1 . Cyber Attacks Against Ethiopian Grand Renascence Dam (GERD).

In June 2020, the Ethiopian Great Renaissance Dam (GERD) became the target of a series of devastating cyberattacks, amid rising tensions with downstream Nile basin countries. According to former INSA chief Shumete Gizaw, these repeated attacks aimed to prevent the dam's construction and initial filling by targeting 37,000 networked computers involved in the project. Allegedly supported by domestic and foreign entities, the attacks were coordinated by Egypt-based hacker groups, including Cyber Horus Group, AnuBis.Hacker, and Security Bypassed, under the slogan 'Black Pyramid War.' The impact was severe: construction was disrupted, the first-round filling of the reservoir was halted, and the operational workflow faced significant setbacks. This not only led to increased costs and delays but also posed a serious threat to Ethiopia's national security and regional stability by jeopardizing water management and energy production. The cyber-attacks exemplify the critical vulnerabilities in national infrastructure and the far-reaching consequences of geopolitical conflicts manifesting in cyber warfare (Ethiopian News Agency, 2021).

2. Cyber Attacks against Ethio -Telecom

In May 2021, Ethio Telecom, Ethiopia's principal and fastest-expanding critical infrastructure experienced a massive cyberattack that lasted over 14 days. The cyber-attacks included attempts at illegal access and distributed denial-of-service (DDoS) attacks, which aimed to disrupt the regular operation of the company's servers by overwhelming them with internet traffic. This sustained attack caused significant operational disruptions, leading to service outages and degraded network performance. Additionally, Ethiopia's ambassador to the European Union linked this cyberattack to the communication outage in the Tigray region in 2020, illustrating the broader implications of such security breaches. The prolonged service disruption likely resulted in substantial financial losses due to downtime and the costs associated with mitigating the attack, while also highlighting critical vulnerabilities in the nation's telecommunications infrastructure. This case underscores the importance of robust cybersecurity measures to protect

essential services from evolving cyber threats and maintain national security and public trust (Nielsen, 2020).

3. Financial Institutions (December 2019)

On December 5, 2019, Ethiopian financial institutions were targeted by a series of massive cybersecurity incidents, leading to a nationwide internet disruption. Ethio Telecom head Frehiwot Tamiru announced that the disruption was a preventative measure taken by the Information Network Security Agency (INSA) to thwart the cyber-attacks. The attacks were sophisticated and coordinated, indicating a significant escalation in the intensity of cyber threats targeting Ethiopia's financial sector. The nationwide internet disruption underscored the critical vulnerabilities within the country's financial infrastructure, potentially causing significant economic loss and eroding public trust in the stability of financial services (Addis Standard, 2019).

4. Cyber-attacks on Ethiopian Airlines (February and August 2021)

In February 2021, Ethiopian Airlines faced cyber-attacks that disrupted its online services, including booking and payment systems. This attack raised serious concerns about data security and the protection of customer information. Further intensifying the threat, on August 21, 2021, Ethiopian Airlines' database system was hacked, leading to a shutdown of the entire system three days later. The disruption limited access to many services, including company email exchanges and other critical server data. The frequency and sophistication of these attacks demonstrate the escalating cyber threat landscape faced by major Ethiopian enterprises, affecting operational continuity and data integrity.

5. Massive Cyber-attack on African Union Data Center (March 2023)

On March 3, 2023, the African Union's corporate headquarters experienced a massive cyber-attack, which caused an emergency shutdown of its data center. The attack rendered services and applications inaccessible, compromising over 200 devices. Monique Nsanzabaganwa, the AU Commission's deputy chairperson, stated that the cyber-attack severely impacted the IT assets within the data center. This incident highlighted the increasing sophistication and impact of cyber threats on critical infrastructures in Africa. The shutdown and service disruption underscore the urgent need for robust cybersecurity measures to protect essential services and maintain operational resilience (Endale, 2023).

These case studies collectively illustrate the increasing intensity, sophistication, and frequency of cyber-attacks on Ethiopian critical infrastructures, causing substantial operational disruptions, economic losses, and undermining public confidence in essential services. The escalating cyber threat landscape necessitates enhanced cybersecurity strategies to safeguard national security and ensure the continuity of critical services.

4.4.2 Case Study: Escalation of Cybersecurity Threats Through Hacktivism in Ethiopia

1. Ethiopian Defense Force Website Attack (July 2015)

During the local political unrest in Ethiopia in 2015, hacktivists attacked and took control of the official website of the Ethiopian Defense Force on July 15. They transmitted political messages reflecting the country's political situation at that time. This incident had profound psychological impacts, sowing fear and uncertainty among the populace. It also tarnished the reputation and image of the Ethiopian Defense Force, undermining national pride and exposing vulnerabilities in the nation's cyber defenses. Social and political tensions were heightened as the attack mirrored and amplified the existing unrest, challenging the government's ability to maintain order and security.

2. Government Websites Defacement Over GERD Conflict (June 2020)

In June 2020, following the construction of the GERD Dam, Ethiopian government websites were frequently defaced by attackers who left messages and symbols related to Egypt. For instance, the homepage of the Ethiopian regional police force training center displayed threats of war over the Nile, with motifs of Egyptian Pharaohs. These attacks had severe political and social impacts, escalating tensions between Ethiopia and Egypt. They created psychological distress among Ethiopians and questioned Ethiopia's sovereignty and ability to protect its critical infrastructures. The explicit threats and nationalistic symbols on the defaced websites struck at the core of national pride, further straining diplomatic relations and social cohesion.

3. Jigjiga University Website Hacked (October 24, 2019)

On October 24, 2019, Jigjiga University's website was hacked, displaying pictures of the Egyptian military and flags. This act of hacktivism aimed to intimidate and provoke psychological distress among Ethiopians, particularly in the context of the GERD conflict. The symbolic display of foreign military symbols on an Ethiopian educational institution's website was a direct challenge to national pride and sovereignty. This attack also had social and ethnic

implications, potentially fueling regional tensions and distrust among different communities within Ethiopia.

4. European Union Delegation Facebook Page Hack (October 31, 2022)

On October 31, 2022, hacktivists took control of the European Union delegation's official Facebook page and posted political messages regarding the armed conflict in northern Ethiopia. This incident caused confusion and mistrust among the public, illustrating the social and psychological impact of such attacks. The EU delegation had to issue a statement advising that the information released on its page should be disregarded, highlighting the political sensitivity and potential diplomatic ramifications of the hack. This incident also underscored vulnerabilities in the cyber defenses of diplomatic missions.

5. Ethiopian Airlines Facebook Page Hack (October 2021)

In October 2021, hacktivists gained control of Ethiopian Airlines' official Facebook page, posting politically motivated messages. This incident disrupted the airline's operations and had significant social and psychological impacts, causing distress among customers and stakeholders. The attack on a major national symbol like Ethiopian Airlines damaged national pride and confidence in one of the country's leading enterprises. It also highlighted the growing sophistication of cyber threats and their potential to disrupt critical services.

6. Ethiopian State Media Facebook Hack (October 4, 2021)

On October 4, 2021, during Prime Minister Abiy Ahmed’s new government inauguration, the Ethiopian Broadcasting Corporation’s Facebook account was hacked, and politically motivated messages were posted. This incident, occurring during a highly symbolic political event, had substantial political and psychological impacts.t undermined the credibility of state media and highlighted vulnerabilities in the country's information security, affecting public trust and national pride.

7. Ethiopian House of Federation Facebook Page Hack (January 30, 2022)

On January 30, 2022, the Ethiopian House of Federation's official Facebook page was hacked and displayed politically motivated messages. This attack on a key legislative body had profound political implications, challenging the institution's integrity and authority. It also contributed to social unrest and psychological unease among the population, reflecting the growing sophistication and intensity of hacktivism in Ethiopia.

8. Ethiopian Press Agency Facebook Hack (March 10, 2020)

On March 10, 2020, the official page of the Ethiopian Press Agency was hacked by cyber offenders who posted politically motivated messages. This attack disrupted the national news dissemination process, affecting the public's access to reliable information. The psychological impact of such an attack included increased fear and uncertainty, while the political implications involved questioning the government's ability to protect its critical communication channels.

These hacktivism cases collectively demonstrate the escalating intensity, sophistication, and frequency of cyber-attacks on Ethiopian websites and social media pages. The damage impacts span psychological distress, social and ethnic tensions, political instability, threats to sovereignty, and diminished national pride, highlighting the urgent need for enhanced cybersecurity measures to protect vital national assets and maintain public trust and stability.

CHAPTER FIVE

DATA ANALYSIS AND KEY FINDINGS

This chapter synthesizes findings from government documents, survey responses, and interviews to interpret the evolution of Ethiopia's cybersecurity threat landscape over the past decade. Using a mixed-method explanatory sequential design, it examines the factors driving these threats and their impact on national security. By aligning these findings with the research objectives and integrating insights from the literature review, the chapter presents a comprehensive academic analysis.

5.1 Cyber security Threat Landscape in Ethiopia over the Past Decade (2013-2023)

The first research question of the study is, "What changes occurred in the trend of cybersecurity threats in Ethiopia over the past decade?" In this section, the findings obtained from multiple sources to find the research question are analyzed and interpreted in the quantitative and qualitative phases, respectively.

In the quantitative phase, the statistical data obtained from INSA demonstrated that cybersecurity threats in Ethiopia have escalated exponentially over the last decade (2013–2023). According to statistical data, cybersecurity threat incidents have increased by 16,322% in the past decade. Local and foreign sources of cybersecurity incidents have been reported differently in terms of their frequency and exposure levels. For instance, the famous cybersecurity company Kaspersky reported that the number of cybersecurity incidents in Ethiopia was 18000 attacks and 30,000 ransomware by 2023 alone (Capital Newspaper, 2023), whereas the local sources used in this study indicated fewer incidents. Furthermore, according to Business Insider Africa, Ethiopia is the third African country with the highest cybersecurity threats (Oluwole, 2023), and based on the research of the famous software company "INTERSOG," Ethiopia is the most sensitive country in Africa for cybersecurity threats (Kateryna, 2023). However, various local sources in Ethiopia have minimized the magnitude of threats and exposure levels (Halefom, 2015; Yirga, 2022). The discrepancies regarding reported cyber security threat levels among external and local sources may stem from variations in reporting styles, data collection and analysis methods, detection capabilities, etc.. Although there is a statistical difference in the magnitude of the threats among various reports, all local and foreign sources indicate an exponential escalation in cybersecurity threats in Ethiopia. In the survey questionnaire, the majority of participants

(95.1%) believed that cybersecurity threats in Ethiopia have escalated significantly over the past decade. The weighted mean of 4.45 also indicates a strong tendency toward the belief that cybersecurity threats have significantly increased in the country in the past decade. This implies that cybersecurity officers in Ethiopia have a common perception of the escalation of cybersecurity threats over the past decade.

In the qualitative phase, cybersecurity experts further explained the previously discussed quantitative data. The interview response indicated that cybersecurity threats are not only increasing in frequency but also in intensity, which implies that high-risk cyber-attacks have risen in the past decade, impacting political, sociocultural, and economic dimensions. The response further indicated that in order to understand the intensity of the threats, in addition to their quantitative measures, they should also be measured qualitatively by considering their impact on sociocultural, political, and economic aspects.

The cases presented in Chapter 4 further indicated the escalation of threats in frequency and intensity, which could be seen by their impact on various aspects of society. Participants also stated that, in the Ethiopian context, the threat level of cybersecurity is growing faster than the advancement of digitalization. This suggests that digitalization has not been protected by a proper security infrastructure. Furthermore, the interview responses indicated that the actual cybersecurity threats in Ethiopia are expected to be more than reported for different reasons, such as the increasing number of undisclosed cyber-attacks and organizations' reluctance to disclose the actual number of incidents due to a fear of losing reputation. Halefom (2015) also stated in his article the under reporting of incidents due to organizational reluctance because of fear of reputation. This implies that the reported data may not reflect the actual threat level and that the probability of unreported cyber incidents is high.

While certain existing literature, such as Yirga (2022) and Yabets (2022), raises concerns about the escalation of cybersecurity threats, this study delves deeper into contextual intensity and implications beyond just quantitative aspects.

Overall, triangulated collective sources suggest that cybersecurity threats have escalated significantly in Ethiopia over the past decade in terms of frequency and intensity. These threats are not merely technical issues, but also multifaceted issues that pose profound challenges to national sovereignty and the integrity and autonomy of the state in the digital age.

5.2 Factors Contributing To the Rise of Cybersecurity Threats in Ethiopia

The second research question investigates the factors that contribute to the rise of cybersecurity threats. According to existing studies, a lack of awareness, budgets, and outdated cybersecurity policies and strategies have been identified as the main driving factors behind the escalation of cybersecurity threats in Ethiopia (Iyasu, 2018; Abenezer, 2019; Yirga, 2022). This study focuses on the main factors that contribute to cybersecurity threats, particularly in the Ethiopian context. This identified factor has not been sufficiently studied in previous literature, so this study attempted to fill this gap by considering the main factors behind the rise of cybersecurity threats, particularly in the Ethiopian context. In this section, the previously presented results regarding the main factors behind the rise of cybersecurity threats are analyzed and interpreted.

5.2.1 Rapid Technological Adoption without Sufficient Cybersecurity Infrastructure

In the quantitative phase, the survey results show that 80.5 percent of the participants believe that rapid technological adoption without sufficient cybersecurity infrastructure is one of the major factors behind the rise in cybersecurity threats in Ethiopia. This high percentage indicates the widespread perception that the lack of adequate cybersecurity measures is directly linked to the escalation of cybersecurity threats. The weighted mean of 3.94 also indicates a strong tendency toward the belief in this statement.

In the qualitative phase, interviews with experts provided detailed explanations of this issue. The interview results indicate that rapid technological adoption without adequate cyber security infrastructure has contributed to the rise of cybersecurity threats in Ethiopia. The response further suggests that the lack of sufficient cybersecurity infrastructure has created a fertile environment for cyber offenders.

This participant's response was corroborated by existing literature. For instance, Iyasu (2018) stated that, nowadays, hackers are shifting their attention to developing countries such as Ethiopia, which have little or no form of protection for newly adopted technologies. Similarly, Yabets (2022) points out that Ethiopia's focus on digital technology has overshadowed the critical need for comprehensive cybersecurity measures, leaving the country more vulnerable to cybersecurity threats. Tewodros (2018) also stated that this factor is the most common contributing factor to the rise of cybersecurity threats in developing countries, such as Ethiopia.

The triangulation of quantitative data, qualitative insights, and existing literature indicates that rapid technological adoption without a proper cybersecurity infrastructure has significantly escalated cybersecurity threats in Ethiopia. .

The interview results also suggested that foreign dependency on digital technologies, particularly security technologies, enhances vulnerability to cybersecurity threats. This dependency is particularly concerning in the realm of security and military technologies, where reliance on external systems can expose the security sector to critical cybersecurity threats, particularly cyberspionage, due to state- and state-sponsored cyber offenders exploiting these vulnerabilities to further their own interests. The theory of the cybersecurity dilemma, as discussed by Buchanan (2016), supports this argument. The cybersecurity dilemma is the concept that states may unintentionally threaten the security and stability of other states by intruding into their vital networks to protect their national security. This theoretical perspective is evident in Ethiopia, where reliance on foreign technologies has increased the country's exposure to state-sponsored cybersecurity threats.

In conclusion, the triangulated data indicate that advanced technological advancement without sufficient infrastructure coupled with foreign technology dependency has contributed to the escalation of cyber security threats in Ethiopia.

5.2.2 Outdated Cybersecurity Policies and Legal Frameworks in Ethiopia

According to the quantitative result, 84.2% of the participants believe that "outdated cybersecurity policies and legal frameworks" contribute to the rise of cybersecurity threats in Ethiopia. This implies that the vast majority of cybersecurity officers believe that outdated policies and legal frameworks contribute to the escalation of cybersecurity threats. This high percentage suggests a broad consensus that current policies are inadequate for protecting against today's sophisticated and volatile cybersecurity threats. The weighted mean of 4.04 also indicates a strong tendency toward the beliefs in this statement. This implies that existing legal and policy frameworks have not kept pace with the recent rapid changes in the cybersecurity landscape, exposing the country to significant cybersecurity threats.

In the qualitative phase, the interview results indicated that outdated cybersecurity policies, legal frameworks, and strategies are among the contributing factors to the rise in cybersecurity threats in Ethiopia. The results further indicate that recent cybersecurity policies and strategies are unsuitable for solving contemporary complex and volatile cybersecurity challenges. The

response also suggested that the absence of cybersecurity in other security policies, such as "Ethiopian foreign affairs and national security," resulted in failure to properly address the issue. Furthermore, the absence of a "national cybersecurity strategy" in the country created fertile grounds for cyber offenders to find and exploit vulnerabilities.

This concern over outdated policies has been extensively documented in the existing literature. Studies by Halefom (2015), Yirga (2022), and Yabets (2022) have consistently stated that outdated policies are major contributing factors to the rise of cybersecurity threats in Ethiopia. Abenezer (2019) also noted that the absence of a national cybersecurity strategy has made Ethiopia more vulnerable to emerging cybersecurity threats.

The triangulation of the quantitative data and qualitative insights, aligned with the existing literature, collectively emphasized that outdated cyber security policies and strategies are a major contributing factor to the escalation of cybersecurity threats in Ethiopia. The combination of these data underscores the clear and pressing need for policy modernization to enhance Ethiopia's cybersecurity resilience.

5.2.3 Local Political Dynamics

The study examined local political dynamics as a contributing factor to the rise of cybersecurity threats in Ethiopia, a significant aspect that has been largely overlooked in the existing literature. Although previous studies have focused on technical vulnerabilities, lack of awareness, lack of budgets, and legal frameworks, this study fills a critical gap by systematically exploring how local political dynamics contribute to the rise of cybersecurity threats in the Ethiopian context.

In the quantitative phase, according to closed-ended survey responses, most respondents (76.9%) believed that local political dynamics were the major contributing factors to the rise of cybersecurity threats in Ethiopia. The weighted mean of 3.87 further indicated that the participants tended to agree with this statement. This suggests a common perception among cybersecurity officers regarding the contribution of local political dynamics to the rise of cybersecurity threats in Ethiopia.

The interview responses indicated that local political dynamics were a significant factor that contributed to the escalation of cybersecurity threats in Ethiopia. The response further indicated that most political groups have recently engaged in cyberattacks to fulfill their political objectives. One piece of evidence supporting this argument is that most cybersecurity incidents increase during prominent political events. This result is further supported by the speech of the

former director of INSA, Dr. Shumete Gizaw, who said during election time and low enforcement operations, cybersecurity threats in Ethiopia are obviously increasing (Ethiopian News Agency, 2021). This observation aligns with the findings of the survey and interviews, suggesting a significant link between political events and the rise of cybersecurity threats.

The results indicated that in Ethiopia, political groups are highly involved in cyberattacks to achieve their political interests; consequently, politically motivated cyberattacks are increasing, and such attacks are highly intense and dangerous, which mostly impacts various aspects of the national security of the country. The case studies presented in Section 4 further confirm this finding. For instance, cyberattacks against Ethio Telecom during the law enforcement operation in northern Ethiopia (Nielsen, 2020) and hacktivism attacks against Ethiopian airlines, the House of Federation, Ethiopian broadcasting corporations, and European Union delegation social media platforms are notable indicators of how local political dynamics have escalated cybersecurity threats in Ethiopia.

The triangulation of mixed-method research, incorporating quantitative data, qualitative insights, and selected case studies, demonstrates a solid and empirically rich evidence base, indicating that local political dynamics significantly contribute to the rise of cybersecurity threats in Ethiopia.

5.2.4 Geopolitical Dynamics

In addition to local political dynamics, this study examined geopolitical dynamics as a contributing factor to the rise of cybersecurity threats in Ethiopia, a significant factor overlooked in most existing literature. In previous studies, Yabets (2021), Yirga (2022), and Alemayehu (2022) mentioned the rise of state-sponsored cyberattacks against Ethiopia following the construction of the Grand Ethiopian Renaissance Dam (GERED); however, there is limited literature exploring the contribution of geopolitical factors as contributing factors to the rise of cybersecurity threats in Ethiopia. This study fills this critical gap by systematically exploring how geopolitical dynamics contribute to the rise of cybersecurity threats in the Ethiopian context using comprehensive approaches.

In the quantitative phase, the results from the closed-ended questionnaire indicated that 81.7% of the participants believed that geopolitical factors were the main contributing factors to the rise of cybersecurity threats in Ethiopia. The weighted mean of 3.94 further indicated that the participants tended to agree with this statement. This suggests that the majority of cybersecurity

officers believe in the contribution of geopolitical factors to the rise of cybersecurity threats in Ethiopia.

In the qualitative phase, the interview response indicated that states and state-sponsored actors are highly engaged in cyberattacks against Ethiopia to fulfill their own national interests. The responses further indicated that these attacks have escalated following the geopolitical tensions that emerged after the filling of the Grand Ethiopian Renaissance Dam (GERD), as stated by Yirga (2022) and Alemayehu (2022). The former director of INSA, Dr. Shumete Gizaw, also raised similar ideas about the relationship between the filling of the dam and the increasing number of high-risk cyber-attacks against Ethiopia. The cases presented in Chapter 4 further solidify this argument by providing more practical evidence. For instance, cyber stacks against GERED-related computer systems, Egypt-based cyberattacks against multiple Ethiopian government websites, and the hacking of the Jigjiga University website displaying the Egyptian military parade are considered significant indicators of how geopolitical factors contribute to the escalation of high-risk cybersecurity threats in Ethiopia.

Moreover, the responses from the interviews indicated that following foreign power pressures and interventions in local affairs, cyberattacks targeted Ethiopian critical infrastructure and core values. The response further indicated that the strategic location of Ethiopia, being in the Horn of Africa, makes it highly vulnerable to cybersecurity threats because of the national interests of the nation states, as various states have vested interests in the region. This indicates the high engagement of countries in cyberspace to fulfill their national interests and the complexity and intensity of cyber threats driven by geopolitical factors.

Theoretically, the realist lens clearly sheds light on this scenario, underscoring the anarchic nature of cyberspace, the domain in which nation-states act only by prioritizing their own national interests, ignoring global norms and collective interests.

The triangulation of mixed-method research, incorporating quantitative data, qualitative insights, and selected case studies, provides solid evidence that geopolitical dynamics significantly contribute to the rise of cybersecurity threats in Ethiopia.

5.3 The Impact of Cybersecurity Threats on National Security in Ethiopia

The third research question of this study is, "How do cybersecurity threats impact the overall national security of Ethiopia?" Before analyzing this question, this study attempted to examine whether the threat actually has an impact on national security by employing multiple methods.

In the quantitative phase, according to the closed-ended survey, 84.2% of the participants believed that cybersecurity threats had an impact on Ethiopia's national security. This response suggests that most cybersecurity officers believe that cybersecurity threats affect Ethiopia's national security. The weighted mean of 4.02 also indicates a strong tendency toward the belief that cybersecurity threats have indeed impacted Ethiopia's national security.

In the qualitative phase of the interview responses regarding the impact of cybersecurity threats, all participants explained the threat's impact on Ethiopia's national security. However, two different ideas emerged among participants regarding the urgency of the threat. Most of the participants believe that cybersecurity threats are "immediate" threats to the national security of Ethiopia and their impact is visible, while others view them as potential threats rather than immediate threats to national security. This discrepancy emerged from the different perceptions of participants regarding the concept of national security. Even though the participants had different views on the urgency of the threats, they all agreed on the general impact of cybersecurity threats on Ethiopia's national security.

Certain existing laws support the critical impact of cybersecurity threats on Ethiopia's national security systems. For instance, Yirga (2022) stated in his study that cybersecurity threats against Ethiopia appear negligible, but that they are practically jeopardizing national security. Yabets (2022) highlighted cybersecurity threats and their impacts on Ethiopia's national security. Furthermore, in post-2018 Ethiopia, cyberspace was considered a military domain by the Ethiopian defense force. Consequently, any attack on Ethiopia's critical infrastructure and sectors through this domain is considered a violation of the country's sovereignty (Yirga 2022).

Moreover, the cases presented in Chapter 4 indicate that cybersecurity threats affect Ethiopia's national security by compromising its core values and national interests.

The triangulation of mixed-method research, incorporating quantitative data, qualitative insights, and selected case studies, indicated that cybersecurity threats have a significant impact on the national security of Ethiopia.

In the following sub-sections, the findings of the research question "How do cybersecurity threats impact Ethiopian national security?" was interpolated in the context of Ethiopian national security.

While some literature stated about the impact of cybersecurity on national security (Yabets, 2022; Yirga, 2022), there is a noticeable absence of research specifically addressing how

cybersecurity threats affect the national security of Ethiopia. This study tried to fill this gap by conducting a comprehensive analysis of how cybersecurity threats impact Ethiopian national security, by using multiple sources and triangulation methods.

5.3.1 Impact of Cybersecurity Threats on National Security: Disruption of Critical Infrastructures

In the quantitative phase, according to the closed-ended survey results, 84.4% of participants believed that cybersecurity threats impact national security by disrupting critical infrastructure. The weighted mean of 3.99 further indicated that the participants tended to agree with this statement. This result suggests that the majority of cybersecurity officers believe in the impact of cybersecurity threats on national security through the disruption of the critical infrastructure.

In the qualitative phase, the interview responses indicated that in Ethiopia, cyberattacks on critical infrastructure are a significant threat to national security by affecting the overall national economy of the country by disrupting daily business activities and production. Furthermore, the response indicated that an effective cyberattack on critical infrastructure could erode public trust in state institutions by dismantling the proper functionality of the government and by calling into question the government's ability to secure critical services.

Furthermore, the cases presented in Chapter 4 indicate that cyberattacks against GERD, Ethio Telecom, and Ethiopian Airlines are considered an indicator of how cybersecurity threats undermine Ethiopia's national security. Beyond service providers, Ethiopian critical infrastructures are sources of national pride, symbols of national dignity, and pillars of solidarity, attacking them by any means considered to directly compromise the national security of the country.

Furthermore, the consideration of cyberspace as a military domain in Ethiopia supports the argument that cyberattacks on critical infrastructure are equivalent to acts of war. Given the centrality of critical infrastructure to national survival and interests, such assaults can pose a significant threat to national security in this digital age. Although the existing literature on this specific issue is sparse, Yabets (2022) supported this argument, stating that a cybersecurity threat could impact Ethiopia's national security by affecting its critical infrastructure.

The triangulation of quantitative data, qualitative insights, and selected case studies indicated that cybersecurity threats could impact Ethiopia's national security by disrupting the country's critical infrastructure.

5.3.2 Impact of Cybersecurity Threats on National Security: Political Dynamics

In the quantitative phase, according to the closed-ended survey questionnaire, 77.7% of the participants believed that cybersecurity threats impact national security by affecting political dynamics. The weighted mean of 3.91 further indicated that the participants tended to agree with this statement. The results suggest that most cybersecurity officers believe in the impact of cybersecurity threats on Ethiopia's national security by affecting the country's political dynamics.

In the qualitative phase, the interview results indicated that cybersecurity threats can affect national security by affecting political dynamics. The results further indicate that, recently, political groups have been engaging in cyber operations to fulfill their political objectives. Consequently, multiple political groups attack various government media platforms and websites to propagate information that reflects their political objectives. Most of the propagated information is intended to trigger conflicts and exacerbate existing political and security challenges faced by the country. The responses further suggested that propagating information through hacked media platforms threatens national security by eroding the social values and solidarity of the people, particularly the politically motivated propagated misinformation that mostly spreads through the hacked government media. This is very dangerous in countries such as Ethiopia, which has multiple ethnicities and diversity.

The cases presented in Chapter 4 indicate that politically motivated cyber-attacks against media platforms affect the political stability, social cohesion, and solidarity of the country, which consequently endangers national security. For instance, the messages transmitted via hacked platforms of the Ethiopian House of Federation, Ethiopian news agency, and Ethiopian Broadcasting Corporation are intended to fuel the existing political disputes and ethnic tensions in the country, which are already threatening its national security. Furthermore, the responses indicated that cybersecurity threats are multiplications of other national security challenges that the country faces, such as ethnic tensions and armed political disputes.

The triangulation of quantitative data, qualitative insights, and selected case studies indicated that cybersecurity threats could impact Ethiopia's national security by affecting its political stability and social cohesion.

5.3.3 Impact of Cybersecurity Threats on National Security: National Sovereignty

In the quantitative phase, according to the results of the closed-ended questionnaire, 75.15 percent of participants believed that cybersecurity threats impacted Ethiopian national security by undermining sovereignty through nation-state attacks. The weighted mean of 3.95 further indicated that the participants tended to agree with this statement. This indicates that the majority of cybersecurity officers are aware of the effect of cybersecurity threats on national security by compromising national sovereignty through nation-state attacks.

In the qualitative phase, the interview results further indicated that recently, foreign actors have repeatedly attacked Ethiopian critical infrastructure and sectors to achieve their national interests and these attacks are clearly considered a direct violation of sovereignty. The responses also suggest that the interference of foreign actors in Ethiopia's domestic affairs through cyber warfare is seen as a direct violation of sovereignty, as it undermines the state's supreme power to manage its affairs without external influence. Furthermore, the response suggested that the security sector's vulnerability to cybersecurity threats due to recent technological advancements could disrupt law enforcement operations, steal sensitive information, and damage the security infrastructure. Such cyber operations have the potential to significantly weaken Ethiopia's sovereignty by compromising internal security mechanisms.

Existing literature has not properly discussed the influence of cyberattacks on the sovereignty of Ethiopia. However, Ethiopian government officials have repeatedly raised the issue of sovereignty in response to the recently escalated cybersecurity threats. For instance, during the 3rd National Cyber Security Month, which was celebrated with the theme "Integrated Cyber Security for National Sovereignty," the issue of cyber security threats and their impact on national sovereignty was highly emphasized (Fana Broadcasting Corporation, 2022). The former Director General of INSA, Shumete Gizaw, PhD, also said that "enhancing the cybersecurity of Ethiopia is inextricably linked with defending its sovereignty." (Fana Broadcasting Corporation 2021).

The cases presented in Chapter 4 further indicate the impact of state-sponsored cyberattacks on the sovereignty of a country. Attacks on critical infrastructure in Ethiopia and the spread of threatening messages against the country are considered direct violations of national sovereignty. Furthermore, the recognition of cyberspace as a military domain by the Ethiopian government

underscores that any attack against the country's critical sectors and core values is considered an act of war that significantly undermines the sovereignty of the country.

The triangulation of quantitative data, qualitative insights, and selected case studies collectively indicated that cybersecurity threats could impact Ethiopia’s national security by undermining its sovereignty.

CHAPTER SIX

CONCLUSIONS

6.1 Conclusions

The aim of this study is to examine cybersecurity threats in Ethiopia over the last decade, analyze the factors that trigger these threats, and examine their impact on Ethiopian national security. Using an explanatory sequential design with mixed methods, this study synthesized findings from government documents, survey responses, expert interviews, and significant cybersecurity incident cases.

Evolution of Cybersecurity Threats in Ethiopia over the Past Decade

The analysis indicated that cybersecurity threats in Ethiopia have increased tremendously over the last decade. Quantitative data from the Information Network Security Agency (INSA) indicate a staggering 16,322% increase in cybersecurity incidents between 2013 and 2023. Survey responses and interviews with experts corroborated these findings, demonstrating that cybersecurity threats are not only increasing in frequency but also in intensity. This implies that high-risk cyber-attacks have risen in the past decade, impacting political, sociocultural, and economic dimensions, emphasizing the necessity of qualitative indicators of these threats in addition to quantitative measures.

Factors Contributing to the Escalation of Cybersecurity Threats

Regarding the factors contributing to the escalation of cyber security threats in Ethiopia, this study focused on less-discussed or overlooked factors in the existing literature. Accordingly, the following factors were identified as contributors to the escalation of cybersecurity threats in Ethiopia.

- **Rapid Technological Adoption**: The study concluded that the rapid adoption of digital technology without an adequate cybersecurity infrastructure has resulted in an increase in cybersecurity vulnerability. Moreover, reliance on foreign technology, particularly security and military technologies exacerbates vulnerability and exposes a country to state-sponsored cyberattacks.
- **Outdated Cybersecurity Policies**: The study concluded that outdated cybersecurity policies and strategies have failed to address current emerging cybersecurity threats, emphasizing the critical need for policy modernization.

- **Local Political Dynamics:** Various political groups in Ethiopia employ cyberattacks to attain their political goals. The rise in cyber incidents following major political events in Ethiopia suggests that internal political dynamics have played a key role in the rise of cybersecurity threats.
- **Geopolitical Dynamics**: This study confirmed that geopolitical factors, particularly those associated with the Grand Ethiopian Renaissance Dam (GERD), have fueled state-sponsored cyberattacks against Ethiopia. Further, Ethiopia's strategic location in the Horn of Africa makes it more vulnerable to foreign cyber operations intended for national interests.

Cybersecurity threat and its implications for national security of Ethiopia

The study concluded that cybersecurity threats have profound implications for Ethiopia's national security, as evidenced by both quantitative and qualitative data, and practical case studies. According to the findings, these threats affect national security in the following ways.

- **Attacks on Critical Infrastructure:** The study confirmed that cyberattacks on Ethiopian critical infrastructure disrupt daily activities and erode public trust in fundamental state institutions. These attacks go beyond disrupting services and further undermine core national values, symbols, and dignity, which are fundamental aspects of national security.
- **Impact on Political Dynamics:** The study concludes that in Ethiopia politically motivated cyberattacks undermine political stability and social cohesion. In Ethiopia, hacked media platforms are used to propagate misinformation, exacerbating ethnic tensions and political disputes, which threaten national security.
- **Undermining National Sovereignty:** This study confirmed that cyberattacks by foreign actors are regarded as a blatant violation of Ethiopian sovereignty. These assaults could undermine the internal security apparatus and law enforcement activities. The Ethiopian government's identification of cyberspace as a military domain emphasizes the gravity of the challenges to national sovereignty. Furthermore, any cyberattack against a country's key infrastructure or fundamental values could potentially be considered an act of war.

This study provides a comprehensive understanding of Ethiopia's cybersecurity threat landscape, highlighting factors that have not been thoroughly discussed in existing literature. By focusing on rapid technological adoption, outdated policies, and the influence of local political and geopolitical dynamics, this study offers new insights into the multifaceted nature of cybersecurity threats in Ethiopia, and their implications for national security.

REFERENCES

Abenezer, B. (2019). *Developing national cybersecurity strategy for Ethiopia* [Master's thesis, Tallinn University of Technology, School of Information Technologies, Department of Software Science]. https://digikogu.taltech.ee/en/Download/06ef8980-905c-4c08-94d1-7918a42e80a0

Alemayehu, T. (2023). State and non-state actors threats to Ethiopia in the context of the GERD dispute. *Intelligence Analysis, CSec6132*.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. Retrieved from Cambridge University Press.

Elsa, T. (2023). Increasing cyber-attacks target Ethiopia. *Abren*. https://abren.org/increasing-cyber-attacks-target-ethiopia/

Federal Democratic Republic of Ethiopia. (2006). *Federal Negarit Gazeta, Information Network Security Agency Establishment Council of Ministers Regulation No. 130/2006, 13th Year No. 5*. Addis Ababa: 24th November, 2006.

Federal Democratic Republic of Ethiopia. (2009). *The National Information and Communication Technology Policy and Strategy*. Addis Ababa: August 2009.

Federal Democratic Republic of Ethiopia. (2011). *Ethiopian National Information Security Policy*. Ethiopian Information Network Security Agency. https://testportal.insa.gov.et/wp-content/uploads/2022/09/National-Information-Security-Policy-2011_compressed.pdf

Federal Democratic Republic of Ethiopia. (2014). *Information Network Security Agency Re-establishment Proclamation, Proclamation Number 808–2013*. Accessed 4 September 2022.

Tewodros Getaneh. (2018). Cyber security practices and challenges at selected critical infrastructures in Ethiopia [Master's thesis, Addis Ababa University]. Addis Ababa University Institutional Repository. Retrieved fromhttp://etd.aau.edu.et/bitstream/handle/123456789/19110/Tewodros%20Getaneh%202018.pdf?sequence=1&isAllowed=y

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections: The Quarterly Journal, 19*(1), 73–86. https://doi.org/10.11610/connections.19.1.07

Horn Review. (2023). Cyber defense: Yet another frontline in Ethiopia's developmental landscape? *Horn Review*. Retrieved from https://hornreview.org/cyber-defense-yet-another-frontline-in-ethiopias-developmental-landscape/

Hough, P., Malik, S., Moran, A., & Pilbeam, B. (Eds.). (2015). *International security studies: Theory and practice*. Routledge.

Human Rights Commission. (2021). Joint investigation by the Office of the United Nations High Commissioner for Human Rights and the Ethiopian Human Rights Commission into allegations of violations and abuses of international human rights law, international humanitarian law and related crimes across Tigray, Ethiopia.

Isnarti, R. (2016). A comparison of neorealism, liberalism, and constructivism in analysing cyber war. *Andalas Journal of International Studies, 5*(2), 151-166.

Iyasu Teketel. (2018). Cybercrime in Ethiopia: Lessons to be learned from international and regional experiences [Unpublished master's thesis]. Addis Ababa University.

Jiri, & Valenta, L. F. (2018). 2007: Russia's Cyber War in Estonia. In *Russia's Strategic Advantage in the Baltics: A Challenge to NATO?* (pp. 24–27). Begin-Sadat Center for Strategic Studies. Retrieved from http://www.jstor.org/stable/resrep16828.19

Kemp, S. (2023). Digital 2023 Ethiopia. DataReportal. Retrieved April 6, 2023, from https://datareportal.com/reports/digital-2023-ethiopia

Lachow, I. (2011). The Stuxnet Enigma: Implications for the Future of Cybersecurity. *Georgetown Journal of International Affairs*, 118–126. Retrieved from http://www.jstor.org/stable/43133820

Yabets Markos. (2022). Cyber security challenges that affect Ethiopia's national security. *Addis Ababa University School of Graduate Studies Department of Political Science and International Relations*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4190146

Ministry of Information. (2002). The Federal Democratic Republic of Ethiopia foreign affairs and national security policy and strategy. *Policy document*.

Misgana Yifru. (2021). Assessment of cybercrime governance in Ethiopia since 2004. *New Media and Mass Communication, 96,* 1-10.

Osawa, J. (2017). The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review, 24*(2), 113–131. https://doi.org/10.1080/13439006.2017.1406703

Samme-Nlar, T. (2020). The Future of Armed Conflict in Africa: What Cyber Attacks on Ethiopian Government Tells Us. *Gefona*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779294

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security, 14*(1), 1-8. https://doi.org/10.5281/zenodo.15924

Skopik, F. (Ed.). (2018). Collaborative cyber threat intelligence: Detecting and responding to advanced cyber-attacks at the national level. *CRC Press*.

Temesgen Aschenek. (2019). The quandary of cyber governance in Ethiopia. *Journal of Public Policy and Administration, 3*(1), 1-7. https://doi.org/10.11648/j.jppa.20190301.11

Yirga Badma. (2022). ሳይበር ደህንነት በኢትዮጲያና ለኢትዮጲያ ብሄራዊ ደህንነት ያለው አንድምታ. FDRE Defence War College EDJISS, 1(1)

Halefom Hailu. (2015, May). The state of cybercrime governance in Ethiopia. University of Oxford.ResearchGate.https://www.researchgate.net/publication/322234805_THE_STATE_OF_CYBERCRIME_GOVERNANCE_IN_ETHIOPIA

Addis Standard. (2022, May 3). INSA says cyber-attack on GERD, financial institutions foiled. *Addis Standard*. https://addisstandard.com/insa-says-cyber-attack-on-gerd-financial-institutions-foiled/

Fana Broadcasting Corporation. (2022, October 11). Safeguarding cyber security one of national priorities: DPM & FM Demeke. https://www.fanabc.com/english/safeguarding-cyber-security-one-of-national-priorities-dfm-fm-demeke/

Business Insider. (2023, March 20). List: African countries most vulnerable to cyber threats in 2023. *Business Insider Africa*. https://africa.businessinsider.com/local/markets/list-african-countries-most-vulnerable-to-cyber-threats-in-2023/zmghfbx

Capital Newspaper. (2023, June 12). Cyber-attacks bombard Ethiopia. *Capital Newspaper*. https://www.capitalethiopia.com/2023/06/12/cyber-attacks-bombard-ethiopia/

APPENDICES

Appendix A: Questionnaire Survey

Dear Respondent,

This questionnaire is an integral part of a master's research project at the Institute of Peace and Security Studies at Addis Ababa University. Its purpose is to investigate cybersecurity threats and their implications for Ethiopia's national security. Your participation is voluntary and confidential, and completing the questionnaire is expected to take approximately 15 minutes. Please carefully consider each question and select the response that aligns best with your views. For inquiries or feedback, feel free to contact the researcher at [mengesha.fentaw@aau.edu.et]. Thank you for dedicating your time and cooperation.

Section 1: Demography

1. What is your highest level of education?
   - ( ) Diploma
   - ( ) BSc
   - ( ) Master's Degree
   - ( ) PhD

2. How many years of experience do you have in cyber-security?
   - ( ) 0-2 Years
   - ( ) 3-5 Years
   - ( ) 6-8 Years
   - ( ) Above 8 Years

3. Do you have any specialized certifications in cyber-security?
   - ( ) No
   - ( ) Yes

Section 2: Cyber-Security Threats in Ethiopia

4. In your opinion, how have cyber-security threats in Ethiopia changed over the past decade?

- ( ) Decreased
- ( ) Remained the same
- ( ) Moderately increased
- ( ) Highly increased
- ( ) Extremely increased

Section 3: Factors Contributing To the Rise of Cybersecurity Threats in Ethiopia

For each statement below, please indicate your level of agreement:

5. Rapid Technological Adoption without Sufficient Cybersecurity Infrastructure

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

6. Outdated Cybersecurity Policies And Legal Frameworks

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

7. Local Political Tensions

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

8. Geo-Political Tensions

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

Section 4: Impact of Cybersecurity Threats on Ethiopian National Security

9. Please indicate your level of agreement with the statement: "Cybersecurity threats have a significant impact on Ethiopian national security."

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

For each of the following statements, please indicate your level of agreement and consider how cybersecurity threats could impact Ethiopian national security:

10. How do you think cybersecurity threats could impact the national economy and security?

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

11. In what ways might cybersecurity threats challenge the sovereignty of the nation and its security?

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree

- ( ) Strongly Agree

12. Consider the potential disruptions to critical infrastructures caused by cybersecurity threats. How does this affect national security?

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

13. Reflect on how cybersecurity threats could influence the political dynamics and the implications for national security.

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

14. Evaluate the impact of cybersecurity threats on the security sectors and their role in national security.

- ( ) Strongly Disagree
- ( ) Disagree
- ( ) Neutral
- ( ) Agree
- ( ) Strongly Agree

Thank you for your participation!

Appendix B: Interview Questions

No.	Interview Questions
1	How has the landscape of cybersecurity threats evolved in Ethiopia over the last decade?
2	What are your thoughts on the consequences of rapid technology adoption without adequate cybersecurity infrastructure in Ethiopia, particularly concerning the escalation of cybersecurity threats?
3	How do you perceive the influence of outdated cybersecurity policies and legal frameworks on the increasing cybersecurity threats in Ethiopia?
4	In what ways do local political dynamics contribute to the growing cybersecurity threats in Ethiopia?
5	How do geopolitical dynamics contribute to the escalation of cybersecurity threats in Ethiopia?
6	What is your opinion on the overall impact of cybersecurity threats on Ethiopian national security?
7	Could you elaborate on how cybersecurity threats specifically affect Ethiopian national security?