COLLEGE OF SOCIAL SCIENCES

DEPARTMENT OF POLITICAL SCIENCE AND INTERNATIONAL RELATIONS

MA in International Relations and Diplomacy

Analyzing the cyber Security and its Capacity Barriers to Ethiopia's Cyber Sovereignty

By Tsion Genene

Advisor Dr. Fekade Terefe

2024/2025

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF SOCIAL SCIENCES

DEPARTMENT OF POLITICAL SCIENCE AND INTERNATIONAL RELATIONS

M.A. PROGRAM IN INTERNATIONAL RELATIONS AND DIPLOMACY

Analyzing the cyber Security and its Capacity Barriers to Ethiopia's Cyber Sovereignty

BY TSION GENENE

APPROVED BY BOARD OF EXAMINERS

Advisor	**Signature**	**Date**
External Examiner	**Signature**	**Date**
Internal Examiner	**Signature**	**Date**

Table of Contents

List of Figures

List of Tables

Abstract

Ethiopia's ability to secure its cyberspace is essential to its strategic pursuit of opportunities in the digital world because, in addition to endangering national sovereignty, a lack of cyber protection will also jeopardize the enormous potential that comes with digital engagement .This study analyze Ethiopia's vulnerabilities to cybersecurity and how they can affect the state sovereignty. Employing a qualitative research approach, the study draws on data from key informant interviews and existing literature. The finding highlighted that Ethiopia's increasing dependence on the digital realm poses a direct challenge to its national sovereignty, largely due to a fragile cybersecurity framework stemming from obsolete technology, insufficient skilled personnel, and inadequate inter-agency collaboration. The nation's weaknesses go beyond simple data breaches, encompassing threats to essential infrastructure and the potential for foreign interference. The study concludes that in order to safeguard its digital future, Ethiopia must promptly implement a strategic and all-encompassing approach, which includes enforcing a national cybersecurity policy, investing in technological advancements and public awareness initiatives, and enhancing its international collaborations to address global cyber threats.

Keywords: Cyber security, State Sovereignty, Ethiopia

Lists of Acronyms

AU	African Union
CCPA	California Consumer Privacy Act
CERT	Computer Emergency Response Team
CIGI	Centre for International Governance Innovation
CISA	Cybersecurity and Infrastructure Security Agency
E4J	Education for Justice
ECA	Ethiopia Communication Authority
ENA	Ethiopian News Agency
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GERD	Grand Ethiopian Renaissance Dam
IBM	International Business Machines Corporation
ICT	Information and Communication Technology
INSA	Information Network Security Agency
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MOFA	Ministry of Foreign Affairs
NCSS	National Cybersecurity Strategies
NIST	National Institute of Standards and Technology
PHI	Protected Health Information

PII	Personally Identifiable Information
R&D	Research and Development
RMF	Risk Management Framework
SLTG	State, Local, and Tribal Governments
SOC	Security Operations Center
UN	United Nations
UNODC	United Nations Office on Drugs and Crime

Chapter One

1. Introduction

1.1 Background of the study

The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. It is also referred to as information technology security or electronic data security (Kaspersky, 2023). Casey Clark (2023) observes cybersecurity is the protection of internet-connected systems from cyber threats. According to Raj Roy (2021) Cyber threats include a wide range of attacks ranging from data breaches, computer viruses, denial of service, and numerous other attack vectors. This study looks at the definition of cyber threats, types of cyber threats, and some common examples of threats.

There was an increasing recognition through the 1990s and the first decade of the 21stCentury that globalization has been tending to complicate the perception of national security (Andy.S, 2010).As Akhil Bhadwal, 2023) notes, cybercrime has evolved significantly since computers were connected to the internet and started sharing messages. Through time, computer users have been appropriately concerned about these risks, even if the amount of risk is significantly more now than it was originally.

Abid A. Adonis (2020) claims the idea of regulating cyberspace through international law is not very novel. The concept of cyber sovereignty, which refers to the ability to create and implement rules in cyberspace, has been discussed by governments and scholars alike. Since 1996, governments, businesses, and legal professionals have all frequently advocated for and opposed international internet law.

ICT penetration and usage are increasing steadily, even though Ethiopia is still falling behind many developing nations. Ethiopia has started integrating ICT use throughout its entire social, economic, and political structures due to the strong evidence that these technologies can lower poverty and promote economic growth. ICT development has been designated as a strategic plan priority by the government (Halefom Hailu Abraha 2015).

Politically motivated cyberattacks and espionage have both been studied and documented for a considerable amount of time. Hackers enter the systems and networks of particular nations, businesses, governments, and highly critical infrastructures by filtering networks in order to steal vital data (Gedion Getahun, 2022).

Additionally, it would be very beneficial if nations talked about cyber issues more frequently. Significant conversations take place, and many nations are not technologically modern. They require assistance in order to take care of themselves, look into and quickly secure their borders, and stay clear of harmful activity. A significant increase in technical capacity is required for this (Gedion Getahun, 2022).

Individuals and businesses use the practice to prevent unauthorized access to data centers and other computerized systems.Cyber security is essential due to the fact that governments, military entities, corporations, financial organizations, and healthcare institutions gather, manage, and retain vast quantities of data on computers and various devices (Juliana, 2023).

As Adnan Kadhum Jabbar Al-Shaibani' s (2020) case study result shows because of the dangers that result from cyberspace conflict, cybersecurity has become a basic requirement that all developed and developing countries strive to achieve; as a result, many countries have resorted to developing strategies to ensure their cyber security.

Cybersecurity is important for national security because it safeguards all types of data against theft and damage,Including Sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and government and industry information systems (Abi Tyas, 2023).

Halefom Hailu Abraha (2015) says; technology is neutral and has the ability to empower both builders and destroyers. Technology, like any new innovation, will always have its detractors who only see its potential for evil and its supporters who only see its ability for good. Cybercrime claims the lives of millions of people and results in losses worth trillions of dollars globally. More than ever, and for a negligible expense, common people can devastate people, businesses, and governments from far-off region.

Reqiq Staff (2023) says Ethiopia's mobile network and telecommunications infrastructure have seen major improvements. Ethiopia's internet penetration rate was 16.7% at the beginning of 2023, and estimates place the country's internet user base increased by 2.6% just in 2022–2023. This is encouraging growth. Modernizing digital payment systems offers significant economic growth potential; in emerging countries, it could raise GDP yearly by 3%. More precisely, it is predicted that by 2025, digital transactions in Ethiopia will have increased nine times from 2020 levels. Similar to national interest, the term "national security" has gained enough traction in the political discourse of international relations to denote a unique policy goal (Arnold, 1952).

The Ethiopian government addressed the implications for national security resulting from the widespread use of ICT in the economy and society in 2009 by adopting a general ICT policy and strategy with cyber security implications (Halefom Hailu, 2015). As we know, Ethiopia was building the Grand Ethiopian Renaissance Dam (GERD). However, the project has faced cyber threats, as evidenced by recent attacks on critical infrastructure activities, including the GERD project itself. NaDa Mustafa, 2021 says The Grand Ethiopian Renaissance Dam (GERD) second filling process was the target of a cyberattack attempt that Ethiopia has countered, according to an announcement made by the Information Network Security Agency (INSA).

The Ethiopian News Agency (ENA) reported on April 28.2022 that the Ethiopian Information Network Security Agency declared that it had stopped cyberattacks coming from Egypt. "The goal of the cyberattack attempts, which took place between June 17 and June 20, was to put Ethiopia under political and economic pressure," (Qamar, 2020) . It’s a good example of an emerging threat to Ethiopia’s national security. The Component strategy of the Ethiopian government regarding cybersecurity, marked by a collection of inconsistent laws, poses a considerable threat to the country's digital sovereignty. As the state endeavors to establish a defense, a troubling lack of awareness among numerous organizations concerning the current governance protocols results in a significant vulnerability. This gap between governmental initiatives and institutional preparedness effectively renders the nation's digital frontiers vulnerable, increasing the risk of cyberattacks that could jeopardize essential infrastructure, diminish public confidence, and ultimately threaten Ethiopia's national sovereignty (Halefom Hailu, 2015).

1.2 Statement of the Problem

Africa is facing a number of Internet-related challenges, including security risks, infringement of intellectual property rights, and data protection. Despite the fact that cyber criminals target people both inside and outside their country, most African governments lack the technical and financial resources to identify and monitor electronic exchanges deemed sensitive to national security (ECA, 2014).

The exponential growth of cyberspace use in Africa is not being matched by the necessary skills. As a result, broad-based education initiatives on Internet safety and security are required to address issues of child protection and social security in general. Furthermore, the facilitation of secure ICT access for users is critical (ECA, 2014).

According to UNODC (2021), many countries and organizations all over the world are battling cybercriminals and working to make systems more secure. However, education is one of the most effective methods of prevention. The Education for Justice (E4J) initiative created a series of cybercrime modules with the help of academics from all over the world.

As Cyber Security and Cyber Resilience in East Africa (CIGI, 2015) report cyber resilience in east Africa can be interpreted in a variety of ways. From a more optimistic perspective, this diversity can be viewed as the result of a successful interaction between international norms that create broad frameworks and establish common standards, national legislation, and practices that adapt and localize these norms in order to ensure their local significance.

The protection of valuable information used for business, nationality information, and critical elements that serve government and society is referred to as information security in Ethiopia. Systems and hardware, for example, aid in the storage and transmission of data (Reba, 2005).

Ethiopia is increasingly vulnerable to cybersecurity threats that jeopardize its sovereignty due to its increasing reliance on digital technologies and the interconnectedness of cyberspace. These dangers have the ability to compromise national security, damage vital infrastructure, lose confidential information, and erode public confidence in governmental agencies. Ethiopia is susceptible to serious cyberattacks that could jeopardize its sovereignty because its current cybersecurity posture is insufficient to counter these threats.

According to Yabets Markos (2022), the major cyber security challenges in Ethiopia that related to a lack of computer technology, a lack of cyber awareness or cyber culture, and a lack of an effective cyber security policy. Also his thesis investigated how these challenges can affect national security by identifying the various causes that contribute to the development of the challenge.

Ethiopia's Current State of Cybersecurity, The country has experienced an increase in cyberattacks due to a number of factors, including inadequate institutional cyber security governance, a lack of knowledge and experience in cyber security, and a lack of standardized legal frameworks. These issues require particular attention (Kibreab Adane, 2020).

The problem this research addresses is the fundamental threat that emerging cybersecurity vulnerabilities pose to Ethiopia's state sovereignty. While the government has implemented disparate pieces of legislation and policy, a cohesive national strategy is lacking. This results in a weak cybersecurity posture characterized by an inability to effectively manage threats, a shortage of skilled professionals, and a pervasive lack of awareness across both public and private sectors. As a result, Ethiopia is inadequately prepared to defend against sophisticated cyberattacks that could compromise its critical infrastructure, erode public confidence, and facilitate foreign interference in its internal affairs, ultimately undermining its sovereign control

1.3 Objective of the study

1.3.1 General objective

To analyzed Ethiopia’s current cyber security situation and its effects on national sovereignty, as well as to make recommendations for ways of strengthening Ethiopia's cyber defenses and protect its interests in the digital sphere.

1.3.2 Specific objectives

-To analyze the most prevalent cyberattack types in Ethiopia and analyze their specific impacts on private companies, government systems, and critical national infrastructure.

-To find out Ethiopia's existing cybersecurity policies, laws, and regulations against established international best practices and standards.

- To identify how Ethiopia can strengthen its cybersecurity capabilities and digital defense posture through strategic international partnerships and collaborations.

1.4 Research Questions

How do the existing cybersecurity vulnerabilities in Ethiopia impact its national sovereignty, and what strategic actions can the country take to strengthen its digital defenses and safeguard its national interests in the digital landscape?

1.4.1 Specific question

1. Which cyberattack types are most common in Ethiopia, and how do they affect private companies, government systems, and vital infrastructure?

2. How do existing cyber security policies, laws, and regulations in Ethiopia compare to international best practices and standards?

3. How can Ethiopia enhance its cyber security capabilities and fortify its digital defense posture through international partnerships and collaboration?

1.5 Core Argument

Ethiopia's efforts to achieve digital sovereignty are seriously hampered by a significant gap between its operationally disjointed cybersecurity systems and those that comply with the law. Although the country has created operational frameworks (CERT, SOC), technical capabilities (AI, block chain defense), and basic laws (such as the Computer Crime Law), systemic implementation problems frequently jeopardize these assets. These shortcomings include a severe lack of human capital (insufficiently trained staff and low public awareness); a failure to prioritize cybersecurity financially and strategically; and pervasive institutional fragmentation, which is typified by inadequate interagency coordination and internal political barriers. According to the study (Abenezer Berhanu, 2019) Ethiopia's cybersecurity is currently lacking in effective measures to combat cyber incidents, which has led to an increase in cybercrime in the nation. This is crucial for ensuring national security, economic prosperity, and overall well-being in the digital age.

Based on a June 2023 report from INSA over 6,760 attempts at cyberattack were made against Ethiopia during the previous 12 months. Above them, about 191 could pose a threat. Cyberattacks still primarily target financial institutions, included ministries and regional offices, as well as security and intelligence, the media, health, and education sectors, as well as important government institutions. Their goals were to interfere with the provision of services and destroy infrastructure (Ethiopian Monitor, 2023).

Because of this, the nation is still extremely susceptible to growing dangers both at home and abroad. Therefore, an immediate strategy shift toward required interagency collaboration, extensive workforce development, and ongoing political and financial commitment to convert policy intent into unified national resilience is necessary to strengthen its digital security posture.

1.6 Significance of the Study

The study provides a timely and essential response to Ethiopia's growing cybersecurity issues. In order to help the Information Network Security Agency (INSA) and other important stakeholders prioritize resources and create more focused defense strategies, the research will offer a thorough examination of the most common cyberattacks and their unique effects on the government, private sector, and vital infrastructure. Importantly, policymakers looking to update legislation will use the comparison of current cybersecurity laws and policies with global best practices as a starting point, and initiatives to improve Ethiopia's digital capabilities will be guided by the suggestions for strategic international partnerships.

1.7 Research methodology

A research methodology helps researchers stay on track by restricting the scope of the study, much like a plan for carrying out research. (Divya Sreekumar, 2023)In other words, research methodology serves as a roadmap for a study and the methodological approach that will be used to conduct it.

1.7.1 Approach of the Study

The proper research methodology, including sampling strategy, data gathering tool, data analysis process, and presentation, was chosen by the researcher while carrying out this investigation. To meet the objective of the research the study employs qualitative research approaches. According

to (F GUIDE, 2005), Qualitative research is a form of scientific research. In general, an investigation that seeks answers to a question, produces findings that were not determined in advance, and produces findings that are applicable beyond the immediate boundaries of the study. This study also adopt Ethnography (Conduct in-depth interviews with key stakeholders involved in Ethiopia's cyber security landscape, such as government officials, cybersecurity professionals, and members of the public) and a data triangulation approaches to Utilizing multiple data sources, such as interviews, Observe the impact of cyber-attacks on state sovereignty, as well as the policies that address cyber security and document analysis, can strengthen the reliability and validity of your research findings.

1.7.2 Sampling Strategy

One effective method for reaching the intended respondents and getting important information from them is non-probability sampling. As Adarsh Kumar (2021) says Nonprobability sampling is a sampling technique in which the identity of the person chosen as a sample from the population. Eight informants in total two from each organization used for this study. So this study use Non-Probability sampling to collect data and it involves Snowball sampling to Identifying informants through referrals from existing participants, building upon existing networks and communities. Four organizations were used for this study.

1.7.3 Sources of the data

The researcher used both primary and secondary sources in this investigation. While the primary sources are found in the data gathered from key informant interviews, the secondary sources included journal articles, newspapers, and websites.

In order to gather data for this study, the researcher conducted interviews. The selection of the respondents is based on their knowledge of the issues and their position. The researcher selects informants from pertinent institutions as a result. The targeted interviewers are from financial intelligence service –Ethiopia, Ethiopian communication Authority, Ministry of Foreign Affairs, and Information Network Security Agency (INSA).

In this study, eight informant interviews are used to gather primary data. The analysis will only consider the information obtained from the interviews, even though relevant published and

unpublished literature, such as books, journal articles, and internet resources, has been discovered.

1.7.4 Data Analysis and Interpretation Procedure

Data analysis is the process by which researchers reduce data to a story and interpret it to gain insights (LeCompte and Schensul, 2010) the process of data analysis aids in breaking down large amounts of data into more manageable chunks. The researcher has employed a thematic approach to data analysis first transcribed the information gathered from key informant interviews and document analysis, after which they categorized the information thematically**.**

1.8 Scope of the Study

This study will Ethiopia's vulnerabilities in cybersecurity: evaluating threats to the country's sovereignty. But it will not address broader issues of cyber security policy or strategy. Also it will not cover all aspects of cyber security, but it will focus on the most critical skills and competencies needed by professionals in this field. While the study aims to analyze how a skilled cyber security workforce can help ensure state sovereignty, it does not delve into specific examples of cyber-attacks and their real-world consequences for Ethiopia. This leaves a gap in understanding the potential severity of cyber threats and how they can directly impact national security and sovereignty. The researcher chose financial intelligence service –Ethiopia, Ethiopian communication authority, Ministry of Foreign Affairs, and Information Network Security Agency (INSA) assessment because the majority of studies center on state sovereignty and the organizations that were the targets of cyberattacks.

1.9 Limitation of the study

The sensitive nature of the subject is the primary limitation. The results might not be statistically generalizable to the larger Ethiopian cybersecurity scene because they were based on eight key informant interviews conducted using non-probability sampling. Furthermore, informants from organizations such as INSA and FIS may be insecure or legally unable to provide specific, direct details about vulnerabilities and classified strategies due to the sensitive nature of national

security and critical infrastructure issues. These conditions could result in information withholding and limit the depth of the analysis on the threat landscape and current policy gaps.

1.10 Organization of the Study

This study paper organized in to five chapters. Chapter one includes an introduction part of the study, background, statement of the problem, core argument, objectives of the study, research questions, significance of the study, scope of the study , research methodology used to conduct the study, and limitations of the study. The second chapter covers a literature review with conceptual and theoretical frameworks for the study. The third chapter presents Ethiopia's current level of cyber security and any possible implications for sovereignty and International partnerships and collaboration. The fourth chapter of the study, on the other hand, will focus the challenges that faced the region regarding cyberattacks and their effect on state sovereignty, and Chapter five will provide a conclusion and recommendation.

Chapter Two

2. Related Literature Review, Conceptual and theoretical perspectives

This chapter includes definitions and explanations of terms used in the study. The definitions and explanations are presented from a theoretical and conceptual standpoint, offering suitable concepts for a thorough analysis of Ethiopia's cybersecurity landscape and guidance to policymakers on enhancing national security.

2.1 Conceptual Framework

2.1.1 What is Cyber Security?

As Sharon Shea (2024), defines Cybersecurity is the practice of safeguarding internet-connected systems, including hardware, software, and data, from cyber threats. Individuals and enterprises use it to prevent unauthorized access to data centers and other computerized systems.

Cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges (Diakun, 2014).

The ITU also defined cybersecurity broadly as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. According to 1st-academy.org (2022) The ISO defined cybersecurity as the "preservation of confidentiality, integrity, and availability of information in the Cyberspace." Personnel, infrastructure, applications, services, telecommunications systems, connected computing devices, and the entirety of transmitted and/or stored information in the cyber environment are examples of an organization's and user's assets (Michael Kelley and Victoria, 2017).

Cybersecurity seeks to protect systems, data, and assets from attacks such as viruses and ransomware, which can hurt enterprises and result in significant financial losses. IBM's 2023

study on the Cost of a Data Breach highlights the rising average cost of catastrophic damages in recent years, with ransomware-related breaches costing considerably more, frequently ignoring the ransom itself. The global economic impact of cybercrime is expected to be enormous in the coming years (IBM, 2023).

According to Halafom (2015), Ethiopia's cyber security governance is still in its infancy. The lack of a comprehensive report demonstrates the precise incidence, consequences, and level of susceptibility of Ethiopia's information society to cybercrime. Therefore, future research on developing Ethiopia's national cyber security governance will be taken into consideration.

According to Alexander S, 2024 Cybersecurity is the discipline of defending against cyber threats against internet-connected systems, including data, software, and hardware. Both private users and businesses use it to guard against illegal access to data centers and other computerized systems.

As Serkan Yusuf (2021), argues attacks by cyber threat actors usually aim to impede research and development, pilfer data for commercial gain, or provide an unfair advantage to rivals. Organizations can preserve their competitive edge and safeguard data and assets by implementing cyber security strategies. Strong security measures aid in shielding a company from possible dangers that might compromise the success of all research and development initiatives. Appropriate cyber risk management is strongly advised because these effects on R&D could have serious repercussions for the organization as a whole.

2.1.2 Digital Identity and Personal Data Protection

Based on Mousam Khatri (2023), Cyberattacks have a profound effect on people that go well beyond the digital sphere. They have an impact on their emotional and financial stability, interpersonal relationships, and level of trust in technology. People need to be proactive and watchful when it comes to protecting their online presence as we continue to embrace the digital age. The likelihood of becoming a victim of a cyberattack can be greatly decreased by utilizing reliable security tools, adhering to strong cybersecurity practices, and remaining up to date on the most recent threats. Furthermore, in order to combat cybercrime and create a safer digital environment for everybody, cooperation between individuals, businesses, academic institutions, and governments is essential. By working together to address the issues raised by cyber threats,

we can create a more resilient and safe digital environment that safeguards everyone's privacy and personal safety.

To reduce the exposure of personal information, one needs to review and modify social media accounts and other online accounts' privacy settings on a regular basis. Organizations are required by law to protect the personal data of individuals, under the terms of numerous data protection laws, including the California Consumer Privacy Act (CCPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Because breaking these laws can lead to hefty fines, it is crucial that companies follow stringent data protection guidelines (Godwin Olaoye, 2023).

2.1.3 State's Sovereignty and Cyber Security

As Pallavi Khanna (2021), when it comes to exercising their "cyber sovereign" states are on Equal Legal Status, This suggests that every state has the equal right to exercise sovereignty over its territory, regardless of its resources. States have the right to exercise their sovereign rights in cyberspace in a manner similar to how they do so elsewhere. However, they must also acknowledge the responsibilities that come with these rights. States have the authority to create any kind of cyber infrastructure they choose thanks to their sovereignty. This is subject to the caveat that states must respect other states' rights when engaging in cyber activities and that they must peacefully resolve cyber conflicts that endanger international peace and security.

As world internet conference report, 2020 In order to conduct operations and uphold order in cyberspace, sovereign states are essential player's one fundamental rule governing international relations in the modern era. The principle and spirit of this agreement extend to cyberspace and cover all facets of state-to-state relations. Each nation has, in reality, extended their national sovereignty into cyberspace, although there are disagreements regarding the concepts and methods of doing so.

According to Baezner Marie (2018), the phrase "sovereignty" is only rarely used by states in their national cybersecurity strategies, and even in those instances when they do use the term, they usually don't define it well and only occasionally. States also don't always have the same definition of the term. Nonetheless, it seems that in the context of cybersecurity, states adhere primarily to the Westphalian interpretation of the concept of sovereignty. Additionally, it seems that the idea of sovereignty is applied to tactics

Based on African Union Peace and Security Council (2024), “Sovereignty is an attribute of States. By virtue of sovereignty, States enjoy, under international law, territorial sovereignty, and supremacy in their internal and external affairs. States are also under an obligation to uphold principles of international law including the duty not to infringe on the independence of other States or to violate their territorial sovereignty.” Also The African Union emphasizes that it must respond to transnational crimes committed in cyberspace using ICTs in compliance with its responsibilities under the UN Charter, particularly those pertaining to the peaceful settlement of disputes and other relevant obligations standards of international law, including the obligation to protect the territorial sovereignty of states (Helal, M 2024).

World internet conference, 2020 report explores the concept of sovereignty in cyberspace, arguing for its extension from a state's physical territory to the digital domain. It defines sovereignty in cyberspace as the supremacy and autonomy a state enjoys over its cyber infrastructure, entities, activities, data, and information within its borders. The core elements of this concept are then elaborated upon:

- **Independence:** States possess the right to self-determination in cyberspace, including choosing their own path for development, governance models, and internet policies, free from external influence.
- **Equality**: Aligned with the principle of sovereign equality in the UN Charter, all states have the right to participate equally in global cyberspace governance and contribute to shaping international rules.
- -**Jurisdiction:** This entails various legal authorities:

-Legislative Jurisdiction: States can enact laws to regulate their cyber infrastructure, entities, activities, data, and information to safeguard national security, public interests, and the legal rights of citizens and organizations within their territory.

-Administrative Jurisdiction: States have the right to manage cyber infrastructure, entities, activities, data, and information within their borders in accordance with established laws, maintaining cyberspace order.

-Judicial Jurisdiction: States can exercise judicial authority over these elements within their territory. Additionally, they have the right to apply internationally recognized legal principles for personal, protective, or universal jurisdiction over specific cyber activities outside

their borders that demonstrably impact them. This enforcement may require seeking assistance from other countries based on principles of self-restraint, courtesy, and reciprocity.

- **Cyber-Defense**: States have the right to develop cyber security capabilities and take lawful and reasonable measures within the UN framework to protect their legitimate cyberspace interests from external threats.

In cyberspace, sovereignty is defined by equality, inclusivity, openness, and respect for one another. Advocating and upholding cyberspace sovereignty does not grant nations carte blanche or license to behave as beggar-thy-neighbor. Diverse methods of enforcing sovereignty in cyberspace are inevitable, and they will remain so for some time to come. The international community's current challenge is to strike a balance between nations' sovereign rights and obligations while upholding national sovereignty. This is necessary to share the rewards and advantages of the digital age while preserving peace and stability in cyberspace (World internet conference report, 2020).

Kiros Assefa (2018) says that sovereignty signifies the possession of uncontested political authority within a territory. This authority allows a state, as the embodiment of sovereignty, to exercise its power unimpeded by external forces. The concept of sovereignty is most evident in the state's unchallenged use of its coercive power, often blurred with the application of law. Examples of this coercive power include enacting laws like conscription, criminal codes, and tax regulations. The state further extends its authority into personal spheres by regulating marriage recognition and enforcing contracts. In essence, sovereignty grants the state the exclusive right to establish laws and the institutions that uphold them, solidifying its position as the ultimate enforcer within its domain.

The recognition of a state by other states is a critical factor in establishing its sovereignty within the international community. Obtaining recognition hinges on, primarily, the possession of a defined territory. However, the concept of territory itself is presented as a fluid social construct, subject to ongoing negotiation and change. The example of the African continent highlights this point. One could argue that the current territorial boundaries were largely determined by the colonial era Berlin Conference of 1884. However, more recent events, such as the secessions of Eritrea and South Sudan, demonstrate how territorial definitions can be redefined, impacting a state's borders and potentially its sovereignty (Kiros Assefa, 2018).

Based on Kinfe Micheal Yilma (2014), Ethiopia has difficulties protecting its expanding digital area. Even though the country's internet penetration rate is low, the government understands that it needs to bolster its cybersecurity. There are currently few laws prohibiting cybercrime, and there are inadequate protocols for their investigation and prosecution. Although a new, more extensive law has been drafted, it still needs to be improved to include international best practices. Although regional states have some authority in this area, the federal government has the authority to regulate cybercrime. The need for a strong legal framework is recognized by national policies, but putting these plans into practice is still a work in progress. Ethiopia is working to strengthen its cyber security overall, but there are still issues that must be resolved in order to respond more forcefully.

The balance of power in society, particularly between the people and the "state," is referred to as sovereignty. The risks of geopolitical conflict, the constant disturbance of digital and big tech, and worldwide dangers like cybercrime, pandemics, and climate change comprise the hard facts. All of these factors do not respect sovereignty and are not restrained by the boundaries that humans have drawn between nations. Disruptions and possibly fundamental changes are occurring in the international system of states (Paul Timmers, 2023).

Although the term "cyber sovereignty" is often ambiguous and frequently used in connection with state authority and autonomy in cyberspace, sovereignty itself is a well-defined idea in international law in 2015, the UNGGE affirmed that governments' use of information and communications technology, including cyberspace, should respect international law and sovereignty rights and obligations.

The UNGGE 2015 report number 27 states that state sovereignty, as well as the international conventions and concepts that follow from it, pertains to how states conduct ICT-related activities and to their authority over ICT infrastructure on their land.

Paul Timmers in his 2023 work, "Sovereignty in the Digital Age," highlights several crucial areas that need to be addressed when examining sovereignty in the online environment. He argues that a comprehensive understanding requires considering various viewpoints on international relations and how the traditional notion of sovereignty is being reshaped by the digital realm. Furthermore, Timmers emphasizes the importance of grasping the complexities of digital technologies and their interconnected systems, as well as analyzing the driving forces behind key players in this space, such as technology corporations.

2.2 Empirical Discussion

2.2.1 Cybersecurity Landscape in Ethiopia

According to Balcha Reba (2005), there are currently no cyber security standards or policies in Ethiopia. There is currently a lack of developed information security law, ethics, and pertinent legislation and regulation pertaining to the management of information in an organization. If these circumstances don't exist, it won't be feasible to come up with trustworthy cyber security problems. Therefore, careful consideration must be given to developing cyber security standards and policies. Additionally, in order to create more secure computing environments in the future, the information security function's staffing needs to rely on the upcoming generation of professionals who possess the right combination of knowledge and expertise to foresee and handle complex information security issues.

According to the Ministry of Information, Press, and Audiovisual Department (2002), "our poverty, backwardness, and the infancy of our system of good governance are the internal threats to our national interests and existence." The threats from the outside are either in conjunction with domestic issues or they take advantage of our weaknesses brought on by internal problems.

The new decree, In line with Federal Democratic Republic of Ethiopia Constitutional Article 55(I), it is hence stated as issued by Ethiopia, may be referred to as "Information Network Security Agency Reestablishment Proclamation No. 808/2013."

According to this proclamation whereas it has become necessary to ensure the security of advancing critical infrastructures and industries of the country that are vulnerable and going to be more vulnerable to an attack due to their reliance on a computer; protect the cyberspace which is created by the local and international computer networking, so as not to be a national security threat; imperative to ensure the security of information, as information is an invaluable social, political and economic asset; it is essential to secure information and critical computer-based infrastructure to ensure the national interest and citizens' right, and it to establish a strong institution that coordinates national efforts to realize the security of information and critical computer-based infrastructures and capable to implement national cybersecurity policy and strategy effectively.

National information security standards are being prepared by the Ethiopian ICT Development Authority. However, in order to direct the development of standards, information security policy

ought to have been created sooner. ICT development programs hardly ever address security aspects because there is a dearth of national cyberspace security policies and related standards. In a similar vein, the Ethiopian Telecommunications Corporation, the country's provider of telecommunication services and network infrastructure, carries out its operations without established national strategic policies and procedures. The Corporation is depending on security components that are suggested by suppliers and system installers instead (Bhupendra Kumar, 2021).

According to Fentaw (2024), Ethiopia's national security is greatly impacted by cybersecurity risks, as evidenced by data and case studies. Attacks on vital infrastructure damage national values and dignity by interfering with daily life and eroding public confidence in important institutions. Cyberattacks with political motivations cause national instability by disseminating false information that exacerbates political disputes and ethnic tensions. Furthermore, foreign actors' cyberattacks breach Ethiopia's sovereignty by endangering law enforcement and internal security. Since cyberspace is now acknowledged as a military domain, these attacks have the potential to be acts of war.

Also major obstacles that critical infrastructures must overcome include a lack of internal knowledge, outdated technology, trouble spotting security risks, and ineffective preventive measures. Data loss from non-mobile resources, inadequate leadership, and a lack of finance are further problems (Getaneh, 2018).

According to World Bank press release, 2023 Ethiopia is one of the last nations in the world to introduce a digitally enabled, foundational ID system at the national level. Current forms of identification, such as birth certificates and IDs issued by local governments, are unavailable to millions of Ethiopians. They consequently encounter obstacles that make it difficult for them to engage in fundamental formal economy activities like opening bank accounts, obtaining health insurance, getting cash transfers and subsidies, requesting official documentation, and more.

2.2.2 Cybersecurity awareness in Ethiopia

Being aware is a mental state that involves paying attention to certain problems and learning about and comprehending certain concepts (Haeussinger, 2015).

According to an ENA report from 2019, despite the nation's growing technological trends, awareness and capacity to prevent cyberattacks remain low. This exacerbates the already dire situation. Among the main issues mentioned are inadequate cyber security governance, legal frameworks, and a lack of awareness. The government and other stakeholders should place a high priority on increasing public awareness and bolstering citizens' and institutions' cyber security capacity.

As Kibreab Adane (2020), research results showed that Ethiopia is experiencing an increase in cyberattacks as a result of the absence of established legal framework to address cyberattacks on an institutional and national level. A majority of Ethiopian government institutions, or roughly 87.4% of them, lack a recognized legal framework to prevent cyberattacks, with only 11.6% of them having legal frameworks that are at the trial stage. The primary sources of cyberattacks are thought to be partners, employees, organized crime, cyberterrorists, and government and non-government sponsored entities. In addition to the absence of uniform legal frameworks, inadequate institutional cyber security governance, a lack of knowledge and experience in cyber security, and a lack of awareness all contributed to the rise in cyberattacks in the nation and demand special attention.

Halefom Hailu Abraha (2015), the fact that victims of cybercrime don't always realize they are being victimized is one of the issues with identifying and looking into cybercrime. In his conclusion, the author recommends that the Ethiopian government and law enforcement organizations raise public awareness of cybercrime, develop practical ways to provide advice on online safety, and promptly notify the public about cybercrime.

Henock Mulugeta(2022) says that the main obstacles to effective cybersecurity in developing nations like Ethiopia include: a lack of regional and national legal frameworks; a lack of comprehensive cybersecurity governance and management frameworks; a shortage of qualified cybersecurity professionals; end users' lack of awareness of basic cybersecurity issues; and a lack of international and national collaboration.

Most Ethiopian banking industries lack cyber security expertise, policies, procedures, and processes for conducting cyber security audits, and there is a low level of preparedness for these audits. Despite the fact that Tesfaye created the Cyber Security Auditing Framework (CSAF) specifically for Ethiopia's banking industry, the framework has not undergone extensive testing. Thus, researchers will continue to strive for its actual application. Only four Ethiopian state and

private banks was the subject of Tesfaye, s attention. Therefore, adding more banks or financial institutions can enhance the framework that has been designed. To increase the capacity of banking stakeholders, a virtual training system or an intelligent security training system must be developed (Tesfaye, 2015).

2.2.3 Related Work

"Cyber Security as an Emerging Challenge to South African National Security" by Griffiths (2016), argues that cyberattacks are a significant and growing threat to South Africa's national security. The main gap it identifies is the lack of a comprehensive national cybersecurity strategy. South Africa has critical infrastructure heavily reliant on information and communication technologies, making it vulnerable to cyberattacks that could disrupt essential services or steal sensitive data. The paper finds that the South African government needs to develop a coordinated approach to cybersecurity, including measures to improve cyber defenses, raise awareness, and deter cyberattacks

Also Kibreab Adane (2020), raised in his research paper ” The Current Status of Cyber Security in Ethiopia” that Ethiopia has no standardized legal cybersecurity framework and a lack of awareness and expertise in cybersecurity. This makes Ethiopia vulnerable to cyber-attacks. Some local researchers are developing cybersecurity frameworks, but they are not rigorously tested.

Ayalew Girma (2016), research assessment of information security culture in the banking industry: The case study of development bank of Ethiopia “assesses that the Development Bank of Ethiopia's (DBE) information security culture. The report identifies several noteworthy vulnerabilities, such as inadequate staff awareness and an official information security policy. The DBE's lax information security culture is revealed by the research to be a worrying vulnerability. Critical bank assets and financial data are vulnerable to cyberattacks, the authors warn. To improve information security procedures within the bank, they advise the DBE to create a thorough information security policy and give employee training programs top priority. To strengthen its overall security posture, the study also recommends that the DBE implement international information security standards.

Jackson Adams, Mohamad Albakajai, (2016) paper “Cyberspace is a new threat to the Sovereignty of the State” discuss that Sovereignty has been regarded as a vital component of the state since its establishment. As a result, the state has worked to uphold its sovereignty over its

regions and has made every effort to safeguard its borders in order to establish its identity. However, the state's sovereignty in preserving its cyberspace faced new difficulties as a result of the technological revolution, which also included advances in telecommunication. Divergent opinions have argued over the existence of cyberspace. On the one hand, some scholars argued that the idea of cyberspace is a libertarian invention that fails to capture the reality of the world. However, some perspectives see cyberspace as a real international space, and as such, any dispute pertaining to cyberspace activities ought to be handled by cyber-jurisdictions.

This paper contends that the shared features of cyberspace are that it is cross-border and poured, regardless of whether it is a "libertarian fantasy" or a "true international space." This renders the conventional methods of defending the state's borders and sovereignty useless. Additionally, the research demonstrates that, despite all the measures the state takes to preserve its sovereignty, cyberspace and its features dematerialization, detemporalization, and deterritorialization can transcend national boundaries. Due to these features, national laws are unable to keep up with the rapid advancement of technology. This argument is supported by case studies from Yahoo, Google, and miditext.com that are discussed in this article. States ought to additionally search for fresh approaches to cyberspace regulation, such as soft law. Legislators and regulators must therefore exercise greater flexibility by granting civil actors a significant role in regulating matters pertaining to e-commerce and cyberspace. The state is able to reserve its framework powers or constitutional prerogatives in this manner.

2.3 Frameworks

Since many agency networks' data were likely compromised, the cyberattack that exploited the Solar Winds vulnerability caused alarms across the federal government. Investigations and mitigations are ongoing to determine the full extent of damage caused by Solar Winds and other recent breaches. In addition to federal systems, state, local, and tribal governments (SLTG) and databases were also affected by the cyberattack. The Solar Winds hacking campaign was "impacting enterprise networks across federal, SLTG governments, as well as critical infrastructure entities and other private sector organizations," according to a statement made on the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) website (Chuck Brooks, 2021).

2.3.1. Risk Management Framework

The possibility that a nation's monetary authority or finance will forego payment of its sovereign obligations, or that it will impose foreign exchange regulations or controls that will substantially reduce or completely eliminate the value of its foreign exchange contracts, is known as sovereign risk (Adam Hayes, 2021).

According to P. Barrett (2018), National Institute of Standards and Technology data the process of continuously detecting, evaluating, and managing risk is known as risk management. Organizations need to know how likely an event is to happen as well as any potential consequences in order to manage risk. Equipped with this data, entities can ascertain the suitable degree of risk to accomplish their goals and communicate it through their risk tolerance. Organizations can prioritize cybersecurity efforts and make well-informed decisions about cybersecurity expenditures by using their risk tolerance information.

A Risk Management Framework serve as a structured template and guiding principle to identify, assess, and reduce risks. The RMF's inception can be linked to the National Institute of Standards and Technology, which created it with the primary objective of protecting the US government's information networks. Additionally, it helps avoid losses such as losing competitive advantages or running afoul of the law (Meeba Gracy, 2023).

By putting risk management programs into place, businesses can quantify and communicate changes to their cybersecurity initiatives. Companies use the Risk Management Framework as a template and set of guidelines to identify, eliminate, and reduce risks. It was first created by the National Institute of Standards and Technology to aid in safeguarding the US government's information networks (Brien Posey, 2024).

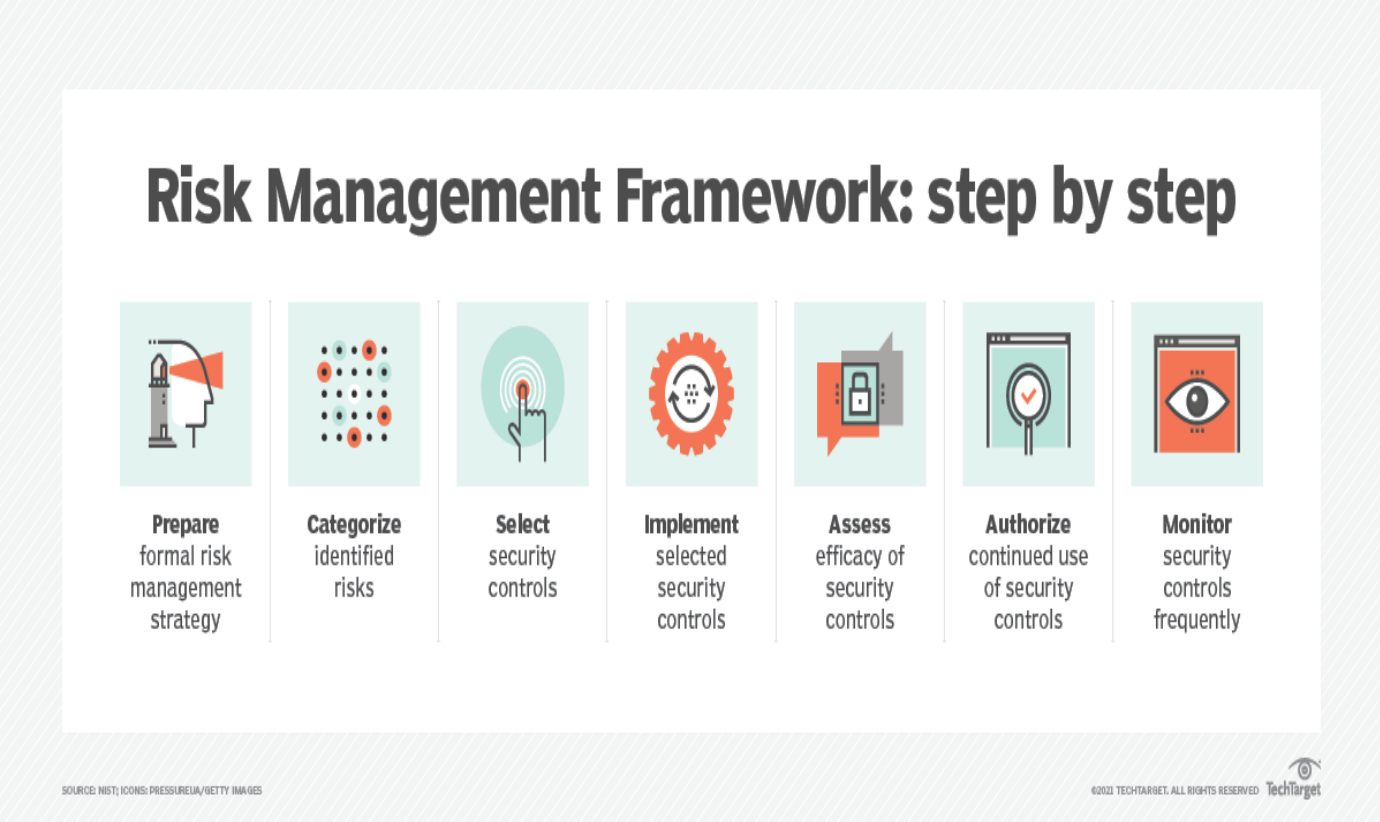

Figure 1: Risk Management Framework Steps

Source: Brien Posey (2024)

Brien Posey (2024), states that the National Institute of Standards and Technology, the following seven steps make up the RMF.

The first one is **Prepared** it's the goal of the RMF's preparation phase is to get the company ready to implement a formalized risk management plan. This could entail figuring out the important risk-management positions and identifying organizational hazards. The second one is **Categorize** this organization start evaluating the risks that have been identified during the categorize stage. This may entail ranking the risks that require attention in order of importance and evaluating the effects of the various risks. The third one is **Select** this choosing the controls that will be applied to safeguard impacted systems in order to reduce or neutralize identified risks is known as the "select" stage. These controls will differ significantly between systems. These could involve developing policies that will help allay worries or adopting monitoring solutions. Based on Brien Posey (2024),, the fourth one is **Implement** the next step in an

organization's risk mitigation strategy is implementation, which begins after the controls have been chosen. Here, the chosen controls are implemented in an attempt to mitigate potential risks. **Assess is** the fifths steps in **risk management** assessment phase follows the application of any chosen controls. It looks to see if the chosen controls were applied correctly and if they are producing the intended outcome. This entails ensuring that any mechanisms put in place are lowering risks in a measurable manner without inadvertently creating new ones. **The authorize stage is** the sixth stage this sometimes linked to the executive's approval of the implemented risk mitigation measures. However, the authorize phase is typically an overview conducted by senior organization personnel who aim to ensure that risk mitigation strategies are effective and compliant with any applicable laws and policies that may be in place within the organization. The last one is **Monitor** according to Brien Posey (2024), The purpose of the monitor phase is to continuously provide situational awareness. It is imperative for organizations to consistently assess their risk mitigation tactics to guarantee their continued efficacy.

For Meeba Grace (2023), cybersecurity risks is one of the example for Risk management framework for every organization, the continuous operation of vital information systems is essential. These systems contain crucial information and features that are necessary for efficient corporate operations. Any interruption or downtime could have serious repercussions.

Including outside vendors in an organization's operations also adds another level of complexity to security. Although working with outside partners has its advantages, there may be security risks involved. These weaknesses may result from a number of things, including insufficient security procedures followed by the third party or the unintentional disclosure of private information while interacting. Therefore, it is essential to thoroughly evaluate a third party's security posture before forming a partnership and to put strong security measures in place to reduce the risks involved in such endeavors.

The Strategy should specify a logical method for risk management that all government agencies and domestic operators of critical infrastructure must adhere to. The strategy should lead to the identification of important resources and services that are necessary for society and the economy to function properly, as well as threats and the risks that go along with them (Guide to Developing a National Cybersecurity Strategy, 2018).

2.3.2 National Cybersecurity Strategy Framework:

African Union, 2018 Workshop for AU Member States discuss about AU Member States on Cyber-Strategy, Cyber-Legislation and Setting up CERTs aiming at providing African Experts with the appropriate Cybersecurity knowledge to prepare and adopt National Cybersecurity Strategies and Cyber legislations. The purpose of the workshop was to provide African Union member states with the information and resources they would need to create their own national cybersecurity policies and laws. Experts from forty African nations were gathered to discuss important topics such as setting priorities, controlling cyber risks, and updating legal frameworks for the digital era. In order to establish a safe and resilient cyberspace for Africa, the emphasis was on advancing a "holistic cybersecurity strategy" that combines stringent laws, technological know-how, and international cooperation.

The Australian Government's Cybersecurity Strategy outlines a comprehensive roadmap to achieve the nation's vision of becoming a world leader in cybersecurity by 2030 (Australian Government, 2023). This strategy prioritizes the protection of Australian citizens and businesses by fostering a more secure strategy which utilizes a multi-faceted approach embodied by six "cyber shields" Each shield represents a critical layer of defense against cyber threats: Strong Businesses and Citizens, Safe Technology, World-Class Threat Sharing and Blocking, Protected Critical Infrastructure, Sovereign Capabilities and Resilient Region and Global Leadership.

Based on this strategy, Australia expects to see the growth and expansion of a strong cyber security sector that contributes to the prosperity of the country, creates high-paying jobs, and finds creative answers to both present and future cyber security needs. A strong market will help cyber security companies by providing them with more chances to win government contracts and funding to spur expansion (Australian Cyber Security Strategy, 2023).

As U.S. Government Accountability Office (2023), observes one of the most important first steps in solving the country's cyber challenges is creating a national strategy. However, for the plan to be successful, it must have precise success metrics and a cost estimate for achieving them. The goal of the strategy is to strengthen cyberspace security and put the US in the best possible position to reap the full rewards and potential of a digital future.

The protection of vital national infrastructure is the unique viewpoint that the Canadian Cyber Security Strategy adopts when discussing national security in cyberspace. This is evident in the three strengthening pillars of the strategy: helping Canadians remain safe online, collaborating to secure all critical cyber systems outside the federal government, and safeguarding government systems. These were primarily intended to counter three types of threats: cybercrime, terrorists using the internet, and state-sponsored military operations and cyberespionage (Government of Canada, 2010).

The European Union Agency for Cybersecurity(2024), also define National cybersecurity strategies (NCSS) as the primary documents used by nation states to establish goals, guidelines, and strategic principles as well as, in certain situations, particular actions to reduce the risk related to cybersecurity.

Depending on the goals of the specific nation and its degree of cyber-readiness, national cybersecurity strategies can take many different shapes and have different degrees of detail. Consequently, there isn't a recognized and widely accepted an explanation of what a national cybersecurity strategy remains (Guide to Developing a National Cybersecurity Strategy, 2018).

Based on Guide to Developing a National Cybersecurity Strategy (2018), the initiation phase, or Phase 1, is the first stage and entails planning the strategy's development as well as identifying pertinent stakeholders and their roles in the process. The assessment of the nation's cybersecurity posture, the identification of cybersecurity threats, and the appraisal of present and potential future cybersecurity risks are all included in the second phase (Phase 2), stocktaking and analysis. The creation of the national cybersecurity strategy is the third phase (Phase 3). This stage entails creating the strategy, getting input from pertinent parties, revising it in light of that input, and publishing it. Phase 4, or implementation, comprises the following: developing an action plan; deciding which initiatives based on the strategy's goals will be carried out; identifying the resources required to carry out these initiatives; and identifying the precise actions to be taken along with the deadlines for completing them. In order to assess the effectiveness (i.e., positive results) and efficiency (i.e., timeliness) of the initiatives, metrics and key performance indicators are also defined during this phase. Phase 5, monitoring and evaluation, aims to ascertain whether the action plan align with the objectives of the cybersecurity strategy. It also assesses the strategy and action plan's suitability for dealing with

evolving cybersecurity risks and their timeliness. Changes are made to the action plan if it is not accomplishing the goals of the cybersecurity strategy. If the strategy is out of date and/or cannot be used to counter new or emerging cyber security threats, changes may also be made to it.

Figure 2: A Guides to Developing a National Cybersecurity Strategy

Source: ITU, (2018).

2.3.3 Linking the frameworks

To understand the theories and how they are applied to the title in an effective manner let's see them separately and how they relate. The first one is National Cybersecurity Strategy Framework (NCSF): This framework sets the national-level goals and objectives for cybersecurity. It helps outline how Ethiopia will address cyber threats and build resilience. The thesis likely analyzes the current cybersecurity landscape in Ethiopia and how it aligns with the NCSF's goals. It also helps to examining if the strategies are effective in protecting national sovereignty.

The second one is Risk Management Framework (RMF): This framework offers a systematic approach to recognize, evaluate, and decrease cyber risks. Utilizing the RMF to examine particular weaknesses in Ethiopia's critical infrastructure or government procedures and Ethiopia's cybersecurity posture and eventually safeguard its sovereignty by being aware of the risks.

The researcher believes that using these two fretworks can provide a comprehensive analysis of Ethiopia's cybersecurity landscape and offer valuable insights for policymakers on how to improve national security.

Chapter Three

3. Cyber-attack and cyber warfare

This chapter provides a comprehensive overview of the cyber threat challenges affecting the country's diplomatic relations and infrastructure.

Beyond awareness problems, cyber dangers present serious obstacles. Successful assaults might cause large financial losses since the attackers may demand ransom payments, steal private data to resell on the black market, or disrupt vital business operations. Additionally, cyberattacks have the potential to damage organizations' reputations and erode public confidence, which may lead to the loss of customers and business partners. Furthermore, such attacks could harm national security by targeting critical infrastructure, disclosing private government data, or interfering with essential services. The wide-ranging consequences of cyberattacks underscore the need for robust cybersecurity safeguards and global cooperation to mitigate these threats.

As Ms.K.Suganya (2022) argues public knowledge of cyber security has been relatively low, and few businesses have made investments in educating the public and raising awareness of cyber security in general. Due to insufficient resources and a lack of management, cyber security is frequently overlooked in budgets since it is given a low priority. Cybersecurity continues to receive little attention from top management, and projects of this nature are not given much priority. This could be as a result of their inaccurate assessment of these risks' impact.

3.1 Challenges of Cyber attack

Based on the 2024 report from the US Government Accountability Office, bank accounts could be drained and private financial information could be posted publicly if the banks we use are targeted. Additionally, you might not be able to report an emergency or ask for help if our communications are interrupted at the same time. The number, intensity, and sophistication of malicious cyberattacks against the federal government and critical infrastructures, including those mentioned above, are rising..

The nation is susceptible to significant cybersecurity hazards due to the lack of a national cybersecurity strategy, which does not provide a solid and integrated defense framework. This strategic deficiency immediately limits an agency's capacity to adequately safeguard government data and systems since agencies often lack the necessary resources, expertise, and contemporary infrastructure. Consequently, disruptive attacks still pose a serious threat to vital infrastructure industries, putting the delivery of essential services at risk. Because individuals haven't made enough of an attempt to safeguard their personal privacy because they haven't been able to completely comprehend or implement the necessary precautions to protect their own digital data, which might act as entry points for more severe cyber threats these concerns are made more complicated.

According to research by Adnan Kadhum (2020) , the threats posed by cyberspace conflicts include internal mobilization against established political systems, use as a tool for internal conflict among the state's components on the basis of sectarian, economic, or religious grounds, the creation of a soft war, the influence of feelings and thoughts, and the start of a psychological and media war, the electronic conflict has evolved into a competition for technological advancements and the theft of scientific and economic secrets. Before it reaches the point where it attempts to control the Internet by attempting to control domain names and addresses, regulating information, and trying to breach national security of nations without the use of aircraft or explosives or even crossing sovereign borders through hacker attacks, site destruction, and espionage, it has the potential to destroy infrastructure and the economy with the same ferocity as a destructive potential of conventional bombing.

Pallavi Khanna (2018) says since cyber activity is one of the challenges that will raise security concerns, the law of self-defense will unavoidably change. Given the growing significance of internet usage in the functioning of society, the law will adapt by providing them with increased protection. By requiring governments to act as responsible users of the cyber domain and lowering the threshold at which cyber operations are deemed to breach the ban on the use of force, the law will increase protection of cyber activities during armed conflicts and empower states to respond strongly.

The largest cybersecurity challenge is protecting your data online, which can be attacked by ransomware, phishing, malware, and other threats. The top 10 rising cybersecurity concerns were listed by Kenanf (2024), along with the major challenges of 2021.

Ethiopia's Data Protection Proclamation No. 1321/2022 serves as the cornerstone of the country's legal response to growing cyber threats. This law is intended to regulate how personal data is processed and safeguarded, establishing the foundation for dealing with threats such as ransomware and phishing. Operationally, the Information Network Security Agency (INSA) is the main government agency in charge of overseeing cybersecurity projects and protecting vital national infrastructure. It is still difficult to properly define the legal standard for what qualifies as a cyberattack that calls for a military-level reaction, which is a key idea in the developing international law of self-defense. As a responsible user of the cyber domain while strengthening its defenses against ever more sophisticated attacks is the state's legal obligation.

The environment of cybersecurity is complex and diverse, with many different attack methods. These include intrinsic defects in software and programming as well as weaknesses in core infrastructure such as hardware, cloud services, and IoT ecosystems. While emerging technologies like block chain and cryptocurrencies present new attack surfaces, persistent threats like malware and scams remain to be a major concern. In addition to external threats, firms also have to deal with insider attacks, which are frequently made worse by inadequate BYOD regulations, and the growing danger of attacks that target or exploit AI and machine learning systems.

Top Cybersecurity Issues Organizations Face by Meeba Gracy (2024), stated that as we all get more interconnected, cybersecurity is becoming more and more crucial. Whether it's sensitive data, personally identifiable information, protected health information, or even your intellectual property, data theft and damage must be prevented. The essay outlines five challenges.

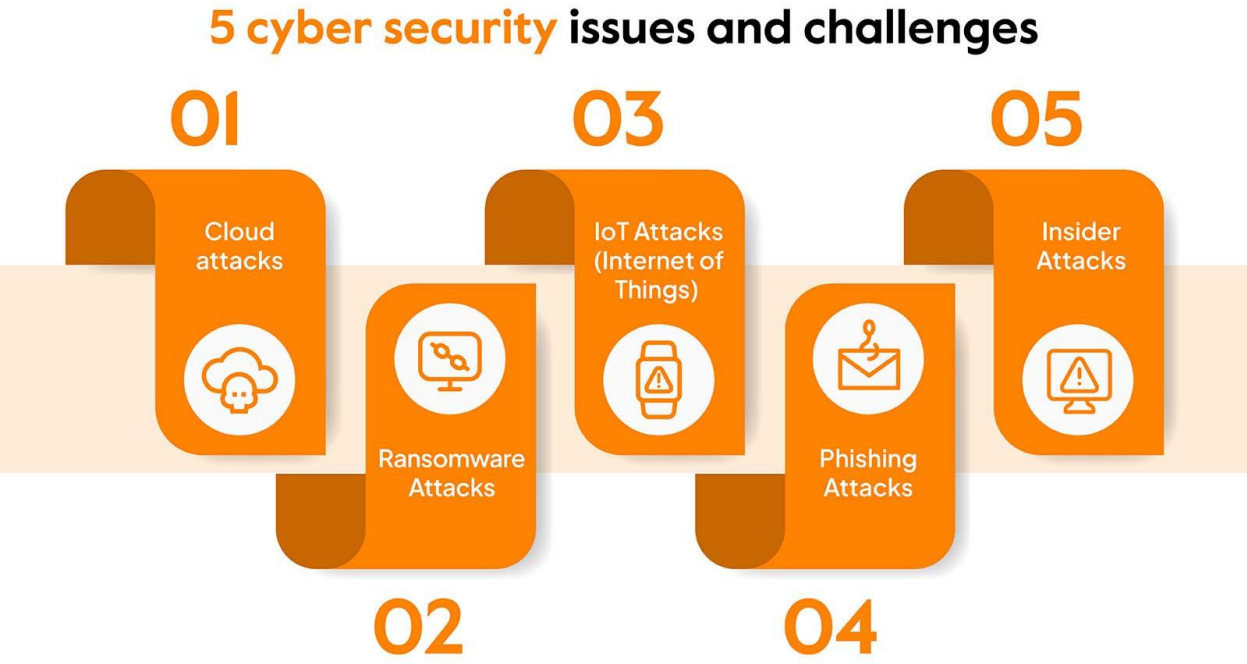

Figure 3: cyber security issues and challenges

The cybersecurity issues facing the government sector will only get more complicated and sophisticated. Some of the major issues that are anticipated to surface in the future are listed below on safe care report (2024)**,** Changing Cyber threats Governments must constantly update its systems to thwart hackers' new methods, strategies, and processes as cyber threats continue to develop and become more sophisticated. Attack surface growth, It becomes more challenging to safeguard all digital assets as the attack surface develops due to increased digitization and the interconnectivity of systems in the public and private sectors, Internet of Things (IoT) devices and other connected technologies as IoT devices and other connected technologies proliferate, government networks become more intricate and susceptible. These devices are very difficult to manage and secure**.** Automation and Artificial Intelligence (AI) while implementing AI and automation-based technologies might improve operational efficiency; they also present new risks and moral dilemmas, such as the use of autonomous systems for surveillance and military applications. Safe care report (2024), also mentioned absence of competent staff Governments find it challenging to recruit and retain qualified workers to address cyber threats because the demand for cybersecurity specialists frequently exceeds the supply.

Conflicts of competence and coordination: It can be challenging to respond swiftly and efficiently to cyber threats when cooperation between various government agencies and the commercial sector is hindered by conflicts of jurisdiction and coordination concerns.

Cyberwarfare and state assaults as countries use espionage, sabotage, and disinformation campaigns to try to obtain a military, political, or economic edge, state sponsored attacks will grow more frequent. Data protection and privacy the gathering and analysis of vast volumes of personal data by governments raises issues about individuals' rights and privacy, necessitating the implementation of appropriate laws and policies to strike a balance between security and individual liberties. International standards and laws governments find it challenging to collaborate and exchange information in order to combat cross-border cyber threats due to the absence of international cybersecurity standards and laws. Global standards and regulations governments find it challenging to collaborate and exchange information in order to combat cross-border cyber threats due to the absence of global cybersecurity standards and regulations. New technology adoption emerging technologies like block chain and quantum computing may cause governments to face new security paradigms and difficulties in safeguarding their data and systems.

Ethiopia is pursuing strong cybersecurity through awareness-raising, cooperation, and ongoing development. The country can strengthen privacy, safeguard its digital assets, and create a robust cybersecurity ecosystem by approaching the issues directly, by increasing awareness, bolstering legal frameworks, testing and validation, and capacity development issues (Adugna, 2024).

3.2 Cyber Warfare

The most common definition of cyberwarfare is a series of cyberattacks targeted at a nation. It has the capacity to destroy civilian and governmental infrastructure and interfere with vital functions, causing harm to the state and maybe fatalities (Yerushalmi, 2023).

Any sort of conflict or war has the ability to affect everyone, whether they are a combatant, a combatant's relative, a civilian, a company, or a nation state. Because of this, studying cyberwarfare is both important and necessary to address the increasing number of problems brought about by this emerging area of conflict. Modern Research on the subject is extensive and covers a variety of subtopics, from attempts to define a cyber weapon exactly to legal concerns

of lawful fight. It can be difficult for someone trying to approach the field of cyberwarfare to grasp all of the difficulties involved, how they relate to one another, the present level of study, and where further research is needed (Michael and Kevin, 2014).

According to Sanjay Goel (2011), *Cyberwarfare is a potent weapon in political conflicts, espionage, and propaganda. Difficult to detect a priori, it is often recognized only after significant damage has been done. Gaining offensive capability on the cyber battlefield figures prominently in the national strategies of many countries and is explicitly stated in the doctrines of several, including China, Russia, and the U.S. It is generally understood they are laying the groundwork for potential cyber conflicts by hacking the networks of adversaries and allies alike. Ethiopia is directly impacted by the global trend of countries giving priority to cyber offensive capabilities since different state and non-state entities can take advantage of Ethiopia's digital weaknesses, undermining its digital sovereignty.*

As defined by John B (2010), which includes the syntactic layer (software, operational instructions), the semantic layer (human interaction, data interpretation), and the physical layer (hardware, cables, satellites). Any of these stages could be the target of an attack, resulting in widespread vulnerability.

Commercial civilian groups have not always been the main targets of hostilities Mohan B (2017), but contemporary cyberwarfare has blurred these distinctions. Highlights how a nation-state employing offensive cyberwarfare combines the destructive purpose of an online criminal, the skill of a traditional hacker, and the indiscriminate reach of an online youngster. Additionally, intelligence and military organizations today have advanced cyber capabilities. This change is especially pertinent to Ethiopia, where recent reports show that vital civilian infrastructure such as financial institutions and major development projects has become a direct target of cyberattacks.

Mohan B (2017), also points out that big nation have a big influence on international arms control and cyberspace regulations. "Every single measure and action [the United States] takes in cyberspace will inevitably have a bearing on the development of international cyberspace arms control in the future." This emphasizes how crucial it is for Ethiopia, a country negotiating

intricate regional and global dynamics, to comprehend the global legal and political environment surrounding cyberwarfare in relation to its own defensive and sovereign capacities.

Also researcher Mohan B (2017),mention that

"As one of the major creators of the international order after World War II, the United States plays an irreplaceable role in international arms control and disarmament. Every single measure and action it takes in cyberspace will inevitably have a bearing on the development of international cyberspace arms control in the future. During my research on cyber-warfare it seemed critical to understand the current situation of cyberspace and then discuss cyber-warfare. Specifically, cyber-warfare's potential to occur in the international community, the restraints on cyber-warfare imposed by existing international laws and, importantly, the potential flaws in these laws"

A cyberattack or series of cyberattacks against a country that have the potential to destroy infrastructure, disrupt essential operations, and cause harm or even death is referred to as cyberwarfare by (Sarit, 2023). Although they are frequently initiated by nation-states, attacks can also be carried out by terrorist organizations or non-state actors in support of adversarial goals. In Ethiopia, where internal political unrest and regional geopolitical concerns might create an ideal environment for cyberattacks intended to weaken the state or destabilize it, this is extremely relevant.

Types of Cyber Warfare Attacks

Sarit (2023), also discuss about 7 types of cyber warfare the most common forms of cyberattacks on his article. **Espionage** in order to steal secrets refers to espionage on other nations. In cyberwarfare, this may entail breaching vulnerable computer systems with spear phishing or botnets before stealing confidential data. So that stealing state secrets, whether through botnets or spear phishing techniques, puts Ethiopia's intelligence and decision-making capabilities at risk. **Sabotage** this is Sensitive information and the dangers of compromise must be identified by government agencies. Terrorists or hostile governments may use insider threats, such as disgruntled or negligent workers or government personnel connected to the attacking nation, to steal or destroy information.

The third types of cyber warfare as Sarit (2023) is **Denial-of-service (DoS) Attacks** by flooding a website with fictitious requests and compelling it to process them, denial-of-service (DoS) attacks block legitimate users from accessing a website. This kind of assault can be used to interfere with vital systems and activities and prevent researchers, military personnel, and civilians from accessing important websites. As capital new (2025) report it emphasizes how complex Distributed Denial-of-Service (DDoS) attacks target Ethiopia's vital sectors, disrupting operations. The Information Network Security Administration (INSA) successfully stopped about 8,854 attempts to do so during the fiscal year 2023–2024. This demonstrates completely that cyberattacks which aim at infrastructure and disrupt operations represent a real threat to Ethiopia's state sovereignty. The otrher is **Electrical Power Grid** Attackers can disrupt infrastructure, disable vital systems, and possibly cause physical injury by targeting the electrical grid. Power grid attacks can potentially interfere with communications and make services like text messaging and communications inoperable.

Attacks by Propaganda a target nation attempts to influence the opinions and feelings of citizens or combatants Propaganda can be used to spread lies to undermine national confidence, reveal embarrassing facts, or align one with enemies. **Economic Disruption** computers are used in the majority of contemporary economic systems. In order to steal money or prevent people from obtaining the money they require, attackers can target computer networks of financial institutions including banks, stock exchanges, and payment systems. **Unexpected Attacks** these are the cyber counterparts of 9/11 and Pearl Harbor. The goal is to launch a surprise, large-scale offensive that will allow the attacker to undermine the enemy's defenses. In the context of hybrid warfare, this might be done to get the terrain ready for a physical assault (Sarit 2023).

Cyberwarfare attacks include Distributed Denial of Service (DDoS), malware, and hacking. Cybercriminals frequently target a variety of vital infrastructures, such as governments, financial organizations, utility corporations, and petroleum businesses. These same attackers aim to damage the very mechanisms that underpin the majority of contemporary economic systems, interfere with vital systems, or steal confidential information. Attacks by cyberwarfare on government infrastructure and networks have the power to influence public opinion and culture. Particularly concerning chances for cyber espionage and disinformation efforts to influence

voters and have a lasting impact on democracy arise in the months and weeks preceding political elections. Andre Slonopas (2024)

Cyber Warfare

Cyberwarfare presents a number of challenges for both attackers and defenders. Attackers are continuously attempting to get over cyber defenses, creating a fast cycle of offensive and defense. In globally, however, the offensive frequently has an advantage. According to John B. (2010), "In a cyberattack, the attacker needs to be successful just once, but the defender needs to be successful often." This is due to the fact that any security has to deal with attacks on large, intrinsically vulnerable networks run by prone human users.

Andrew Krepinevich (2012),on cyber warfare “NUCLEAR OPTION?” book mentioned that depending on the nature of the attack and the attacker’s characteristics, it may be important to test these exploits in an environment as close as possible to the actual target. This may be especially important where the attacker is trying to create catastrophic effects. In such instances, the attacker (assuming it is the government of a state) may risk large-scale retaliation from the defender in the wake of the attack. The risks may be worth it to the attacker if the prospective benefits of the attack are likely to be realized. Mapping the computer network infrastructure of a nation’s critical infrastructure sufficiently to enable a cyber-attack that triggers catastrophic consequences seems likely to require the services of a highly capable intelligence apparatus, the kind only major nation-states can afford to assemble and maintain.

According to fortinet (2023), report the Most Notorious Cyberattacks in History have been uncountable cyberattacks over the years, the following instances of cyberwarfare have had a major influence on the nature of cyberattacks and how nations and businesses protect themselves from attackers.

Cyber warfare in Ethiopia

Nova (2021), Ethiopian Airlines reported a cyberattack on its Facebook page, where a bogus statement purporting to be about the shipment of weapons to Eritrea was published. The account was promptly reclaimed by the airline, which claimed it was "temporarily compromised." After a CNN investigation that claimed Ethiopian Airlines smuggled weapons, the airline rejects the allegations and maintains that it complies with aviation laws.

According to Zelalem (2022) reports, Egyptian hackers attacked a number of Ethiopian official websites in retaliation for the ongoing conflict around the Grand Ethiopian Renaissance Dam (GERD). The June 2020 incident intensified the bilateral tensions between Egypt, which depends on the Nile for its water supply, and Ethiopia, which views the project as essential to growth.

Ethiopia is becoming an important target for ransomware and other exploits due to an increase in cyber threats. Financial, energy, and government organizations in Ethiopia were the targets of DDoS assaults by a hacking collective at the beginning of 2023. In 2023 alone, the nation had over 18,000 ransomware occurrences and 30,000 attacks, which resulted in data loss and service interruptions. Despite efforts to prevent them, these attacks, which have both regional and global origins, pose serious risks to critical infrastructure and national security (Teshome, 2023).

Elsa Tessema (2023) the five countries with the highest average monthly ransomware encounter rates in 2018 were Ethiopia (0 77 percent), Mongolia (0 46), Cameroon (0 41), Myanmar (0 33), and Venezuela (0 31). During that time, each of these countries had an average monthly ransomware encounter rate of at least 0.31%.

According to Teshome, M (2023) capital Ethiopia report during the final nine months of the 2022–2023 fiscal years, the Information Network Security Administration (INSA) responded to 4422 cyberattacks and attempted attacks nationwide, there were gaps because 4,272 of these were appropriately addressed, while 150 caused damage.

Xinhua (2024) Over 4,550 cyberattacks have been stopped by Ethiopia in the first half of the current fiscal year 2023–2024.Xinhua (2024) said that

"Had the cyberattacks succeeded, Ethiopia could have suffered over 10.5 billion Ethiopian Birr (about 186 million U.S. dollars) losses,"

Ethiopia had over 18,000 confirmed attacks and 30,000 ransom ware cases in 2023 alone. This represents a significant increase over the 5586 cyberattacks that were documented in 2021–2022. In general, these attacks aimed to disrupt government and corporate internet services, preventing users and customers from accessing them for hours at a period, sometimes for days or weeks, Amin explained. "It stopped more than 97 percent of all cyberattacks," In 2022, cyberattacks targeted financial institutions and large-scale projects, such as the computer systems of the Grand Ethiopian Renaissance Dam (GERD), which downstream nations, especially Egypt and Sudan, are concerned will eventually reduce their historic water shares from the Nile River, according to a media report from INSA. Subterranean evidence has also been found that Ethiopian people and organizations have been the target of various cyber threats, including ransomware, data leaks, and theft of personal information (Elsa Tessema, 2023).

As Teshome, M (2023), noted Ethiopia has seen a wide range of cyberattacks in recent years, ranging from sophisticated attacker organizations using cloud computing to typical cybercriminal gangs targeted by the nation. “It was discovered that some of these attacks originated locally, while others were worldwide."

According to a report by the Ethiopian news network the attacks are intended to steal information, deny services, and undermine public confidence in the government. The studies also claim that certain forces, particularly those looking to capitalize on the nation's political turmoil and insecurity, are responsible for the attacks. Another factor contributing to cyberattacks is the geopolitics of water (ENA, 2023).

Both attackers and defenders in a cyberwar face numerous difficulties. Both sides must deal with a quick cycle of offensive and defense, and cyber attackers must defeat cyber defenses. Nevertheless, since any defense must deal with attacks on massive networks that are fundamentally weak and operated by human users who are vulnerable to error, the offense is

dominant in cyberspace. In a cyberattack, the attacker needs to be successful just once, but the defender needs to be successful often (John B, 2010).

Considering the data presented Cyberwarfare differs from conventional conflict in that it poses a distinct set of difficulties for states. Because cyberattacks frequently lack obvious attribution, unlike physical combat, it can be challenging to identify the perpetrator and raise hostilities. Furthermore, because cyberattacks are non-kinetic, they may result in low-intensity, protracted confrontations that strain diplomatic ties and undermine international confidence. Furthermore, critical systems are susceptible to cyber disruptions due to the interconnection of contemporary infrastructure, which could have an effect on vital services like healthcare, transportation, and energy. This highlights the broad consequences of cyberwarfare by having the potential to cause societal unrest, economic instability, and even mortality.

Chapter Four

4. Cybersecurity Vulnerabilities and Resilience in Ethiopia

Ethiopia's resilience initiatives and cybersecurity weaknesses, as stated by institutional specialists interviewed for their expert opinions. While highlighting ongoing policy reforms and capacity-building activities, it draws attention to significant issues such technological dependence, low awareness, antiquated systems, and lack of coordination will be discussed in this chapter.

4.1 Current State of Ethiopia's Cyber Infrastructure:

Key informant 1 discusses vulnerabilities arising from a lack of thorough assessment, the relatively recent engagement with cyberspace, and imported technology. Sectors highlighted include banking, telecommunications, and government infrastructure. The informant indicates the complexity in providing a precise evaluation of the government's cybersecurity posture, suggesting a lack of comprehensive data or agreed-upon metrics. This implies that official reports may not fully capture the reality of the situation [1](Interview, September 2024).

Key informant 6 also added the respondent highlighted major structural deficiencies that contribute to cybersecurity threats [2](interview, September, 2024). He highlighted the alarming lack of clear protocols, particularly cybersecurity frameworks, throughout vital infrastructures, as well as the prevalent misapplication of security mechanisms. Furthermore, the assignment of underqualified personnel, which exacerbated the problem of human error, was also identified as a major contributor due to a lack of supervision. As he put it, the widespread use of outmoded systems throughout the nation exacerbates these flaws and increases the risk of misuse.

As the key informant 4 [3](interview, September, 2024), argues that a key cybersecurity weakness is the significant lack of public awareness, which he attributed to 60-80% of attacks. He mentioned reduced technological engagement as a contributing factor. Furthermore, the

[1] Key informant 1: Hibamo Ayalew is international relation officer at the MOFA .Interview, September, 2024.

[2] Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

[3] Key informant 4: Anonymous source from INSA. Interview, September, 2024.

informant also highlighted underinvestment in cybersecurity infrastructure and human resources, compounded by electricity and internet challenges.

Based on key informant 2[4](interview, September, 2024), mentions many of these threats seem to originate outside our borders, often targeting our financial systems and individuals with frequent transactions. As he argues when it comes to government infrastructure, it's more often seen as sabotage, not necessarily a "cyberattack" in the formal sense, at least according to official conclusions

Key informant 4 [5](interview, September, 2024), points out the current technological dependency also exacerbates the conflict. The lack of focus on working as a continent and the lack of consistent procedures, laws and policies are the causes of vulnerability. The lack of capacity among countries makes them unable to work together and makes them vulnerable. The lack of legal action also increases vulnerability.

According to the data, there is a multi-layered, systemic failure in cybersecurity that stems from both governance and technical shortcomings. The use of outdated technology and the lack of defined procedures and structures in crucial areas are vulnerabilities. Human issues, such as the misuse of current security, high rates of under qualification among workers, and a crucial lack of public awareness, significantly worsen these structural flaws. The nation is vulnerable primarily to external threats due to its internal fragility and underinvestment, a situation that is made worse by irregular regional cooperation and the challenge of accurate appraisal brought on by a lack of data.

4.2 Cyberattack Landscape in Ethiopia:

Ethiopia ranks second globally and Africa's top destination for cybercrime, according to Check Point's June 2024 Global Threat Index. South Africa and Egypt are less attacked but other African nations like Zimbabwe, Angola, and Kenya are high-ranking. The most prominent malware used against sectors like government, finance, utilities, and education in the continent of Phorpiex, Expiro, Qbot, and FakeUpdates. Cyber-attacks continue to present a major risk despite

[4] Key informant 2: Anonymous source from MOFA. Interview, September, 2024.

[5]Key informant 4: Anonymous source from INSA. Interview, September, 2024.

attempts to bolster defenses, and therefore it is a matter of necessity that African companies have sophisticated threat intelligence along with good response plans (Sibanda, 2024).

[6](Key informant 1, interview, September 2024) Financial institutions throughout the world were seriously threatened by the WannaCry ransomware. Wegagen Bank and Hibret Bank were among the banks in Ethiopia that were allegedly at risk of suffering losses of up to 3 million Birr, despite the fact that these organizations did not openly admit any direct compromise. This demonstrates the difficulties with attribution and transparency in the wake of cyberattacks in the country's financial system.

As key informant 4 [7](interview, September 2024) Ethiopia is vulnerable to espionage, state-sponsored attacks, and the theft of private data about banking systems, military projects, GERD, and megaprojects. There is a risk to critical infrastructure, such as banks, electricity grids, hospitals, airports, and telecommunications, which might cause economic upheaval and erode public confidence in government agencies. He also mention these dangers impact the nation's economy and day-to-day activities, but they also pose questions about digital sovereignty, particularly when national interests are compromised by cyberattacks or foreign influence. Ethiopia's ability to safeguard its digital realm is crucial to preserving its independence, governance, and social stability as conflict and power dynamics move online.

National sovereignty is threatened by cyber vulnerabilities as [8](key Informant 5, interview, September 2025) states that which compromise security and result in financial damage. When foreign calls bypass Ethiopian networks, especially when they break international communication rules, it might be difficult to intercept and trace them. By limiting law enforcement and exposing users to a range of risks, this emphasizes the wider effects on national security and control.

[6]Key informant 1: Hibamo Ayalew is international relation officer at the MOFA .Interview, September, 2024.

[7]Key informant 4: Anonymous source from INSA. Interview, September, 2024.

[8] Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.

[9](Key Informant 6, interview, September 2025) also added that even though DDoS and telecom fraud are problems, Ethiopian telecom hasn't had a major cyberattack. But as was already indicated, poor planning puts the public's trust at risk in addition to serious data and financial losses. Despite the lack of previous significant events, it is said that even two data breaches might seriously impair operations and damage reputations, exposing vulnerability.

The Ethiopian financial industry is also vulnerable to cyberattacks. [10](Key informant 7, interview, September 2024) stated financial intelligence tracks cyber fraud perpetrators and stolen money for recovery and prosecution, highlighting the financial sector's vulnerability. An institutional investigation into a bank attack revealed multiple actors and how the bank became vulnerable by analyzing financial activities and money flow, indicating a focus on understanding exploitation methods.

Imported technology risks and human error represent key cybersecurity challenges in Ethiopia. [11]Key informant 3 (interview, September ,2025) reveals Ethiopia's cybersecurity vulnerabilities stem from reliance on imported, potentially Unexamined technology, risking data leaks and undermining technological sovereignty. Despite legal and training efforts, gaps remain. He also mention 'Human error, due to limited cyber knowledge leading to risky behaviors like installing malware or inadequate antivirus, further amplifies cyberattack risks, particularly on sensitive systems'.

Ethiopia, a major hub for cybercrime, is also at risk from cyberattacks, with live malware targeting critical sectors. Previous incidents like WannaCry affected banks, and there are still significant problems with the government, the financial sector, and critical infrastructure, even though some industries, like telecommunications, have been severely targeted thus far. The nation is still threatened by espionage and state-sponsored assaults, which erode public trust and national sovereignty. This calls for the prompt implementation of sophisticated threat

[9]Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

[10] Key informant 7: Mulugeta Temesgen Supervision and compliance Directorate director from Financial Intelligence Service-Ethiopia. Interview, September, 2024.

[11] Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

intelligence and cooperative response strategies in order to deal with the novel and complicated cyber threats.

4.3 Ethiopia's Cybersecurity Framework: Implementation Issues and Global Alignment

As highlighted by [12]Key informant 1 (interview, September 2024) despite the lack of a single international legislation, Ethiopia's cybersecurity regulations, such as the Personal Data Protection Proclamation that is in line with the EU's GDPR, are based on international norms. He also mentions Ethiopia instead adheres to regional and international frameworks such as ISO standards and the AU Cyber Security Conventions. Ethiopia wants to improve coordination by signing treaties with more than 50 nations, but its laws need to be updated often to reflect changing cyber threats.

[13]Key informant 3 (interview, September 2024) also added that due to the lack of a single international legislation, Ethiopia is dependent on regional frameworks like the AU Cyber Security Conventions, even though its cybersecurity laws are in line with international standards like the EU's GDPR and ISO guidelines. Ethiopia has ratified international treaties with more than 50 nations in an effort to improve coordination. To keep up with changing cyber threats, its legal framework must be updated on a regular basis. [14]Key informant 4 (interview, September 2024) agreed on the idea and also states that when it functioned as its own ISP in 2004, there was a policy in place to ensure security. Since then, laws like the Personal Data Protection Proclamation, Emergency Proclamation, and Technology Products Proclamation have been established, and a modified policy was approved on June 20, 2016. Ethio-CERT is vital to enforcing these rules and protecting the nation's cybersecurity infrastructure under INSA.

Similarly, Ethiopia's legislative and policy frameworks have made significant strides, as seen by its score of 20 to 28 on this year's International Cybersecurity Index. Ethiopia has established a strong foundation and is making steady progress, even if it still trails behind industrialized

[12]Key informant 1: Hibamo Ayalew is international relation officer at the MOFA .Interview, September, 2024.
[13]Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

[14]Key informant 4: Anonymous source from INSA. Interview, September, 2024.

regions like the EU. By updating legislation, improving education, and pursuing international collaboration, the nation continues to address institutional difficulties and has developed inclusive cybersecurity plans for 2025 and 2030 that are in line with international norms [15]Key informant 5 (interview, September 2024).

Ethiopia's cyber weaknesses are a product of a mix of security measures and outdated, borrowed technology. Well-meaning people can fumble through cyber unawareness and security measures in organizations Create vulnerabilities that expose them to it. It is difficult to have a complete picture of the country's readiness in curbing cyber threats without in depth analyses.

On a global scale, Ethiopia works with the United Nations' worldwide Telecommunication Union (ITU), which establishes worldwide standards and offers security advice for telecom companies. The nation collaborates with ITU teams on a number of cybersecurity initiatives to enhance systems, like creating a Certificate Authority to guarantee safe, unchangeable communication for public services. Due to a lack of local expertise, this entails using open tenders to collaborate with seasoned overseas partners. To close current gaps and conform to international cybersecurity requirements, such collaboration must be strengthened [16]Key informant 6 (interview, September 2024).

Ethiopia's cybersecurity legislation complies with regional and international norms, although it needs to be updated frequently to handle new threats. To increase capacity and enhance coordination, the nation collaborates with more than 50 countries and institutions such as the ITU. Despite advancements, there are still issues with knowledge, regulations, and enforcement, necessitating continued action to improve cybersecurity.

Risk management strategy, as describes by Payne (2022) Creating a plan is one thing, but carrying it out is quite another. A successful risk management strategy should be implementable and incorporated into your day-to-day activities.

[15]Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.
[16]Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

The process involves identifying cybersecurity risks, which include evolving threats and gaps in expertise, evaluating current controls such as existing laws and international cooperation, and implementing ongoing mitigation strategies such as regular updates, capacity building, and stronger enforcement. It shows a continuous process of recognizing vulnerabilities, managing them through collaboration and policy development, and adapting to new risks to reduce potential harm.

[17] Key informant 2 interview, September 2024), Significant barriers impede Ethiopia's progress in cybersecurity, demanding that cyberspace be prioritized alongside physical sovereignty. These challenges are fundamentally institutional, stemming from three main problems: a lack of finance, ambiguous policy frameworks, and a shortage of skilled human resources. Although digitization efforts are underway, security remains deficient across government sectors, including the Ministry of Foreign Affairs (MOFA). Overcoming these issues requires a long-term outlook and increased national aspirations, along with the active involvement of youth. Ultimately, the successful implementation of efficient and well-coordinated national cyber frameworks is essential to translate policy discussions into effective defense, a necessity underscored by the protracted delay in adopting the draft policy.

There is one specific aspect of the policy that needs to be enhanced. As we have been working on it and it has been changing, it must keep up with technology. While we think the current policy is acceptable, there may be a gap if it is not updated regularly. We'll be sad if we find a gap, but we won't be able to put it into practice in time [18]Key informant 3(Interview, September 2024).

As [19]Key informant 5 (interview, September 2024), observes Ethiopia is updating its twelve-year-old foundational text cybersecurity draft to address evolving threats and adapt to a multi-operator telecom environment. Previously focused on Ethio-Telecom, the revised policy now considers risks from multiple carriers like Safaricom. It emphasizes the role of regulatory bodies

[17]Key informant 2: Anonymous source from MOFA. Interview, September, 2024.
[18]Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

[19]Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.

in setting security standards and calls for coordinated protection measures to strengthen defenses across all operators.

Ethiopia's cybersecurity strategy is currently developing and does not incorporate economic factors. Stronger inter-institutional collaboration and a more proactive, all-encompassing strategy are needed. As Key informant 4 [20](Interview, September 2024) Ethiopia's present cybersecurity policy is still in its infancy and has several short comings; most notably that it ignores economic factors. Coordination with other institutions is required, and improvements are frequently only addressed after implementation. As problems arise, the policy is anticipated to be revised continuously, underscoring the need for a more proactive and all compassing approach.

[21]Key informant 4 (interview, September 2024), sates many government organizations are unaware of the importance of investing in cybersecurity and continue to handle sensitive data using antiquated techniques. Crisis response is hampered by inadequate interagency coordination brought on by an over-reliance on INSA, particularly with Defense and Intelligence. This underscores the need for more defined responsibilities and improved cooperation.

According to the viewpoints of the main informants, Ethiopia's current cybersecurity scenario is marked by a notable discrepancy between the effectiveness of its domestic implementation and its conformance with international legislation, which has a direct influence on national sovereignty. Although the country is actively seeking international cooperation with more than 50 nations and organizations like the ITU, as well as establishing a foundation of policies such as the GDPR-aligned Personal Data Protection Proclamation and adherence to AU and ISO standards, these efforts are hampered by a number of systemic issues. Importantly, implementation is hindered by underinvestment in finance and personnel, a lack of qualified staff, and poor inter-institutional coordination, all of which require prioritizing cyberspace like physical sovereignty. The policy framework also suffers from vague guidelines and insufficient economic considerations. Ethiopia must adopt a proactive, long-term strategy that guarantees the

[20]Key informant 4: Anonymous source from INSA. Interview, September, 2024.
[21] Key informant 4: Anonymous source from INSA. Interview, September, 2024.

ongoing modernization of laws and the efficient, coordinated enforcement of frameworks across all crucial sectors in order to strengthen cyber defenses and safeguard national interests. To improve cyber defenses and protect national interests, Ethiopia has to implement a proactive, long-term plan that ensures continuous legal modernization and effective, coordinated enforcement of frameworks across all important sectors.

4.4 Strengthening Ethiopia's Cybersecurity:

INSA constantly strives to increase its team members' capacity. It operates by bringing in college students who train and get experience in order to earn certifications. Even if it depends on how often we use it, many higher education institutions outside of the institution, such as Addis Ababa University, have begun to provide courses. Their goal is to develop trained human resources in the field and to improve the abilities of those who already possess them. [22](Key informant 3, interview, September 2024)

Additionally [23]Key informant 5(interview, September 2024) highlight the Communications Authority's workforce lacks the necessary skills and abilities. Specialists are needed for all kinds of work; therefore even if they have begun to be deployed in different locations, this is insufficient and needs to be addressed. Given the significant global trends and risks we are witnessing, we must be capable and ready. There are not enough human resources, in my opinion. It is essential to plan training, give people authority, and offer acknowledgment in order to close this gap.

[24]Key informant 2, interview, September 2024) agreed and added that due to a lack of training and capacity building, Ethiopia's Ministry of Foreign Affairs is facing a significant cybersecurity a deficient. The majority of staff still communicates formally over unprotected channels like WhatsApp, and none of them have received any cybersecurity training. He also said that outdated techniques are still prevalent, and safe digital technologies are not well understood.

[22]Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

[23]Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.

[24]Key informant 2: Anonymous source from MOFA. Interview, September, 2024.

Effective application and security of government data are nevertheless hampered by a lack of awareness and training, even in the face of new rules like digital signatures.

The Ethiopian Communication Authority, according to Key Informant 6 [25](Interview, September 2024), recognizes the shortcomings of present professional abilities while highlighting the possibilities for workforce improvement. The informant cautions that the government's inability to create a nation and institution that is ever-changing will have dire repercussions.

States have the courage to fight each other for sovereignty. The participation of foreign powers in the affairs of other actors or their allies and beneficiaries has been a defining feature of major wars and conflicts in the twentieth and twenty-first centuries. (Haber Topor, 2023)

According to [26]Key Informant 1 (Interview ,Sept. 2024), Ethiopia's cybersecurity is undermined by a lack of prioritization and enthusiasm for digital competence development, he mentions evident in the insufficient training of diplomats, inadequate basic security for sensitive data, and an overburdened, under-resourced IT department, all contributing to a significant vulnerability to cyber threats.

Ethiopia has made some steps, but its lack of infrastructure and capacity raise serious worries about its ability to identify attacks. Key Informant 3 [27](Interview, Sept. 2024), also there are still a lot of gaps, particularly in law enforcement, despite the efforts of some authorities. Under the current system, it is especially challenging to identify and effectively respond to attacks coming from other nations.

There are currently no legally enforceable international cybersecurity norms; instead, the majority of current activities are headed by the UN, including the Secretary-General. Although these issues are intended to be addressed in the next "Summit of the Future" in December, work has been halted due to the lack of agreement among nations. It is challenging to enforce

[25]Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

[26]Key informant 1: Hibamo Ayalew is international relation officer at the MOFA .Interview, September, 2024.
[27]Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

standards and effectively address new cyber threats in the absence of established protocols. [28](Key Informant 1, Sept. 2024)

As [29](Key Informant 3, Sept. 2024) Despite lacking a policy that outlines how to do so, INSA attempts to address cyberattacks through international means. As permitted by law, when the incident has happened and action has been taken, legal action will be conducted against the attacker.

In addition to limited detection and response infrastructure, a lack of focus on digital capacity, and vulnerabilities in law enforcement responses, especially when it comes to foreign attacks, Ethiopia's cyber security is not strong. The absence of international cybersecurity laws makes matters worse. Despite occasional international cooperation after attacks, there is no comprehensive preventative policy.

4.5 Legal Strength and Operational Fragmentation

Cyber threats can cause serious damage if not addressed proactively. While Ethiopia has strong legal frameworks like the Telecom Fraud Law, Computer Crime Law, and a revised National Cybersecurity Policy, the key challenge lies in implementation. Institutions vary in how effectively they use these tools. [30]Key Informant 4 (Interview, Sept. 2024), He also added the country has established a Cyber Emergency Response Team and a Security Operations Center that monitor threats 24/7. Public awareness and training efforts are also underway to build cyber capacity and reduce vulnerabilities, but consistent, practical application across sectors remains essential.

[31] (Key Informant 8,(Sept. 2024) explains that using an in-house system are not only prevents major cyber-attacks, but also protects Ethiopia from many attacks by deploying a block chain

[28]Key informant 1: Hibamo Ayalew is international relation officer at the MOFA .Interview, September, 2024.

[29]Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

[30]Key informant 4: Anonymous source from INSA. Interview, September, 2024.

[31] Key informant 8: Anonymous source from Financial Intelligence Service- Ethiopia. Interview, September, 2024.

system with banks that is encrypted and visible only to us, so we have done a good job of preventing them from being leaked when we first developed our software.

Both Safaricom and Ethiopian Telecom use automated AI-based solutions to keep an eye on and safeguard their networks. Beyond promoting use, there isn't any coordinated effort, and each operator uses its own cybersecurity procedures in the absence of a common national framework. [32](Key Informant 5, Sept. 2024)

According to [33]Key Informant 3(Interview, Sept. 2024) both international and locally produced tools, such as popular technologies like Metasploit and Wireshark, are used to stop cyberattacks. Metasploit is one of the most popular tools for threat identification and penetration testing, even though Wireshark is free. To improve the efficacy of security, certain tools are kept secret.

While Ethiopia has strong cybersecurity law and operational structures like the CERT and SOC, a primary weakness lies in the uneven application across organizations. While some sectors host state-of-the-art in-house and AI-driven security mechanisms, and both local and international tools are employed for protection, the absence of a unifying national framework means piecemeal and possibly less effective cybersecurity arrangements.

4.6 Interagency Fragmentation and the Imperative for Coordinated Digital Defense:

In cybersecurity, collaboration refers to the combined efforts of the public and commercial sectors to stop, identify, and address cyber threats. Governments, commercial enterprises, and other stakeholders must exchange knowledge, resources, and experience in order to bolster collective defenses against more complex and pervasive cyberattacks. While private companies own most of the vital infrastructure and technical know-how, public entities frequently have the authority to regulate and conduct intelligence. They may enhance early threat detection, lower risks, and create a more robust digital environment by cooperating through sharing threat intelligence, conducting joint investigations, and adopting shared standards. (Prodaft, 2024).

---

[32]Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.

[33]Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

The [34](Key Informant 5, Sept. 2024) states communication authority are working together with other organizations to ensure that every online connection we make is authentic and not tampered with by humans. We are working on a project that requires us to work closely together and we are working well. [35](Key Informant6, Sept. 2024) also added that they collaborate on infrastructure and other matters, engage discussions, and share knowledge with INSA. In order to close the knowledge gap that we require, we also collaborate actively. This gives them permission to collaborate on cyber-related matters.

One common misconception regarding cybersecurity is that INSA is exclusively in charge of safeguarding public service infrastructure, which is frequently the most susceptible connection. The Ministry of Defense and National Intelligence are two important entities with which coordination is unclear as well as blocked by internal politics or a fear of losing power. Although MOFA and INSA coordinate quite well, there is still a lack of interaction with other agencies, and INSA has to clarify its position in order to enhance interagency cooperation. [36](Key Informant 2, Sept. 2024)

When it comes to responding to cyber incidents, INSA is crucial because it is the first to look into and evaluate the problem. [37](Key Informant 7, Sept. 2024) highlighted by tracking financial movements to find the culprits, financial intelligence collaborates closely with INSA, particularly when assaults target financial systems. Additionally, INSA creates tools specifically for these organizations and keeps an eye on systems to identify and stop possible cyber threats.

Information on cybersecurity collaboration is limited, mainly between INSA, communication authorities and financial intelligence on financial crimes. Unclear responsibilities, internal politics (particularly in defense and intelligence), and limited understanding of INSA's unique

[34]Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.

[35]Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

[36]Key informant 2: Anonymous source from MOFA. Interview, September, 2024.

[37]Key informant 7: Mulugeta Temesgen Supervision and compliance Directorate director from Financial Intelligence Service-Ethiopia. Interview, September, 2024.

responsibility, however, impede wider interagency cooperation and halt a single national response.

According to the National Institute of Standards and Technology collaborative risk management enhances threat awareness and response capability, while its absence weakens the resilience of the entire networked environment. (Cichonski et al, 2012).

[38]Key Informant 6 (Interview, Sept. 2024), mention that because of a lack of cooperation and an emphasis on institutional or personal agendas rather than national objectives. Institutions frequently take unilateral action when concerns emerge rather than working together to find answers, which can lead to problems getting worse on a national scale. To properly handle these issues, interagency collaboration and shared accountability must be strengthened.

Lack of institutional collaboration in putting the laws and policies in place is a major obstacle to assuring cybersecurity. Despite the fact that the regulator offers oversight, training, and guidance, many institutions are reluctant, which results in obvious gaps. He also highlight under order to tackle this, initiatives are currently under progress to enhance cooperation and enhance adherence via cooperative dialogues and ongoing supervision [39]Key Informant 3 (Interview Sept. 2024).

[40]Key Informant 6 (Interview, Sept. 2024) strength this concept by focusing on collaboration must be strengthened and national goals must take precedence over institutional or individual agendas in order to improve efforts. And argued more targeted, well-coordinated, and efficient solutions to cybersecurity issues would be made possible by the creation of a specialized working group made up of professionals from pertinent organizations. Continuity, shared responsibility, and effective problem-solving are guaranteed by this team approach.

---

[38]Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

[39]Key informant 3: Abdu Mekonnen is an investigation and development unit, cyber Diplomacy and political affair division officer at INSA. Interview, September, 2024.

[40]Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

Ethiopia is working on cybersecurity. Despite the existence of reaction teams and legislative frameworks, ineffective collaboration among agencies and unequal implementation undermine strong defense. Even though some companies are offering more protection, a single national policy and improved cooperation rates are required to tackle the evolving nature of cyber threats.

From a risk management perspective, Ethiopia has elevated and fluctuating cyber risks with discernible treatment mechanisms (laws, CERT, SOC) but without coherent implementation and poor risk identification, evaluation, and unified control measures due to a fragmented national structure and poor interagency coordination, and thus a more integrated and uniformly enforced strategy is needed in order to successfully counteract its cyber risk exposure.

Coordination of cybersecurity is complicated by the difficulties of integrating organizations and obtaining quick replies. Delays in communication impede development despite attempts like letters and searches, particularly when jobs are urgent and need for prompt teamwork. [41](Key Informant 5 (Interview, Sept. 2024).

[42]Key Informant 2 (Interview, Sept. 2024), also add that the main problem faced in collaboration is that many institutions are unwilling to implement the issued policies, leading to visible gaps in cybersecurity efforts. However, steps are now being taken to address and improve these challenges.

Although MOFA is protecting both digital and physical assets, it is still mainly concentrating on the former. Simulations and scenario-based training are not currently available. Our policies are weakened by the dearth of cybersecurity knowledge, particularly in academic institutions. With antiquated systems still in place, we're lagging behind our neighbors. [43](Key Informant 1, Sept. 2024) and the paper is used for even the most basic tasks, such as processing visas. Real development is limited in the absence of knowledgeable specialists.

---

[41]Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.

[42]Key informant 2: Anonymous source from MOFA. Interview, September, 2024.

[43]Key informant 1: Hibamo Ayalew is international relation officer at the MOFA .Interview, September, 2024.

INSA is making a commitment to improve relations. [44](Key Informant 4, Sept. 2024) have developed an operational system based on ISO 9001/2015 "because we recognize that we will confront obstacles and feel it is our responsibility to work toward implementing them. Although it has been changed, that was not the case previously".

Prioritizing the national interest in solving the issues at hand, cooperating, and carrying on with current efforts are what we need to be improved. People will be able to collaborate in a working group as a result, which will make it easier for them to concentrate on the problems. They will be able to work more intently if a group of subject-matter experts is assembled from each institution. [45](Key Informant 5, Sept. 2024)

[46](Key Informant 6, interview, Sept. 2024) agrees and adds the idea that as a nation, we must work toward a shared objective and stance that is not merely a theoretical plan but is actually achievable. It would be really helpful, in my opinion, if they could develop anything that could lead to a shared understanding and work on how to handle the problems should they arise.

Based on the data of informants Ethiopia places emphasis on digital security but lacks training and possesses national cybersecurity expert deficiency, which slows down policy and sustains aged systems. Certain improvement and standardization are practiced, but this kind of progress is required on a wider national scale, with more interagency coordination through expert groups, and common, applied cybersecurity strategy with clear-cut incident response.

Ethiopia's financial isolation has so far shielded it from many global cyber crises. Major attacks like those on Google or the English stock market didn't affect us because our system is closed and less integrated internationally. However, as we begin integrating with the global market, cybersecurity challenges will grow. INSA and other institutions are strengthening defenses through measures like national ID protections, encryption, and AI use, but we're still behind global standards. Our banking system remains partly manual, limiting attacks so far, but as

[44]Key informant 4: Anonymous source from INSA. Interview, September, 2024.

[45]Key informant 5: Natnael Taddese is a Head of Infrastructure security division at ECA. Interview, September, 2024.

[46]Key informant 6: Taddese Getachew Interner resource management desk officer at ECA. Interview, September, 2024.

digitization increases, improving cyber defenses is critical to reduce vulnerabilities and keep pace with global risks. [47](Key Informant 8, interview, Sept. 2024)

As stated in this chapter Ethiopia's prior financial isolation has offered a degree of protection from global cyber threats, as major international cyberattacks have largely bypassed the country due to its closed and less integrated financial systems. However, this is changing as Ethiopia increasingly integrates with the global market, which is expected to amplify cybersecurity challenges.

Furthermore, Ethiopia is actively working to strengthen its cyber defenses through initiatives like national ID protections, encryption, and the use of AI. Despite these efforts, the country still lags behind global cybersecurity standards. While the banking system's partial reliance on manual processes has limited its vulnerability to cyberattacks so far, the increasing digitization of this sector necessitates a critical and urgent focus on enhancing cybersecurity to mitigate emerging risks and align with global security practices.

[47]Key informant 8: Anonymous source from Financial Intelligence Service- Ethiopia. Interview, September, 2024.

Chapter Five

5. Conclusion and Recommendations

5.1 Conclusion

This study has analyzed cyber security in Ethiopia to protect the state's sovereignty. the complex field of cybersecurity vulnerabilities and resilience in Ethiopia by using contemporary literature and expert knowledge.

It has identified the far reaching effect of cybersecurity threats on the national security of Ethiopia beyond data breaches to include attack on critical infrastructure, erosion of public trust, and political instability due to disinformation. The necessity to counter such concerns is also compounded by the reality that cyberspace is an imagined war battlefield, as foreign cyber-attacks would compromise Ethiopia's sovereignty and potentially endanger law enforcement and internal security.

Ethiopia's weakness in cybersecurity exists in a number of relevant areas of vulnerability. The proactive elimination of security risks and detection are circumscribed by a lack of in-house know how and predominance of outdated technological infrastructure. Inefficient preventive steps, the risk of data loss from non-mobile assets, inefficient leadership, and ongoing budget limitations complicate these shortcomings. While the growing use of technology generates the possibility of progress and expansion, it makes it difficult to expose the country to advanced cyberattacks.

Moreover, the existence of legacy systems and ignorance about general best practices in terms of cybersecurity gives ample room for exploitation. The lack of adequate coordination among the participating organizations makes it difficult for the country to act feasibly against cyberattacks in a cohesive and effective manner.

Ethiopia's sovereignty is threatened simultaneously with these vulnerabilities. The country's capacity to secure its cyber borders, maintain control of its critical infrastructure, and protect its data integrity can all is undermined by cyber-attacks. Declining public confidence in the

government and the risk of foreign interference in internal affairs also undermine sovereign control.

Ethiopia continues to make efforts to enhance its cybersecurity resilience in the wake of these significant challenges. Policy changes and capacity-building interventions are ongoing, demonstrating a desire to harden the nation's defenses. Proactive moves toward a more secure digital world include the rollout of national ID protections, the use of encryption technology, and the examination of artificial intelligence for security applications.

In order to address these issues and protect the sovereignty of Ethiopia, collaborative efforts by many stakeholders are essential. The government must prioritize cybersecurity through the allocation of adequate resources, having well-defined and regularly revised policies, and promoting cooperation among agencies. Constant risk assessment should be carried out, security measures should be implemented, and cybersecurity infrastructure should be invested in by the public and commercial sectors. Schools play an important role in educating the public and building cybersecurity competencies. Acquiring best practices, gaining technical support, and coordinating responses to international cyberattacks all require international cooperation.

Interestingly enough, because of its less integrated financial system, Ethiopia's long-standing financial isolation has unbeknownst to it supplied it with some protection against large scale international cyberattacks. As the country becomes more entwined within the world economy, though, this pillar of protection is weakening. While integration into the economy is essential to growth, it will contribute to the amount and sophistication of cyberattacks. The banking industry's limited reliance upon human operations has so far prevented its vulnerability to cyberattacks. But the rapid digitalization of the financial sector necessitates greater and more pressing emphasis on improving cybersecurity measures in accordance with international security standards in preparation for potential vulnerabilities.

Last but not least, the current cybersecurity posture of Ethiopia is characterized by a significant disparity between strong legal objectives and dispersed operational capability, which seriously compromises national digital sovereignty. Ethiopia must move from a reactive, policy-heavy approach to a proactive, unified national strategy that prioritizes the ongoing modernization of its legal frameworks, requires urgent interagency coordination (getting past institutional politics),

and makes consistent, strategic investments in human capital to effectively enforce its policies across all crucial sectors to fortify defenses and safeguard national interests. The rapid digital integration of local and international markets necessitates this coordinated strategy to mitigate the growing cyber threats.

5.2. Recommendations

A state must have effective cybersecurity in order to preserve its digital realm, govern its cyber borders, and protect its national security. A clear and coordinated plan needs to be developed in order to truly strengthen Ethiopia's cybersecurity posture and protect its sovereignty online. First , a national cybersecurity policy with a specific framework for interagency coordination and information sharing, funding sources, regularly updated legal and regulatory frameworks, ongoing risk assessment, and threat intelligence programs must be established and rigorously enforced.

Second, significant funds must be allocated to awareness and capacity building initiatives, public awareness campaigns, specialized professional training, and the integration of cybersecurity education and training into academic curriculum.

Thirdly, it is necessary to improve technological capabilities and infrastructure by pushing innovative security technologies, upgrading obsolete systems, and creating Security Operations Centers (SOCs).

Fourth, in order to request technical assistance, participate in international cooperation against cybercrime, and exchange threat information, active participation in regional and global collaboration is necessary. Ethiopia can significantly strengthen its cybersecurity resilience, protect its national sovereignty online, and advance a secure digital environment by diligently implementing these recommendations.

References

Abraha, H. H. (2015). The state of cybercrime governance in Ethiopia. ResearchGate. Retrieved from .

Adane, K. (2020). The current status of cyber security in Ethiopia. Social Science Research Network.

Adonis, A. A. (2020). International law on cyber security in the age of digital sovereignty. E-International Relations.

Affairs, A. G. (2023). 2023-2030 Australian Cyber Security Strategy .

Agency, I. N. (2013). Proclamation No 808 2013 Information Network Security Agency.

agency, I. t. (2018). Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity - ITU Hub. .

Asfaw, T. (2018). Cyber security auditing framework (CSAF) for banking sector in Ethiopia. Academia.edu.

Asrat, A. (2024). Cybersecurity in Ethiopia: challenges and opportunities. Ardiland Institute of Technology. p. ArdiLand Institute of Technology.

Assefa, S. K. (2018). Sovereignty, legitimacy and fundamental rights as limitations to criminalisation power of the state. Mizan Law Review . pp. 12(1), 127.

Baezner, M., & Robin, P. . (2018). Cyber sovereignty and data sovereignty. CSS Cyber Defense Trend Analyses, 2.

Bala, B., Kumar, B., Gangone, S., & Kumar, B. . (2022). Cyber security in African Union and Ethiopia and its anticipation. ResearchGate. .

Bhadwal, A. (2023). The history of cyber security: A detailed guide .

Brooks, C. (2021). A risk management cybersecurity imperative for state, local & tribal governments. Forbes. .

Canada, G. o. (2010). Canada's cyber security strategy. Public Safety Canada.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. . (2012). Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-61 Revision 2). . *National Institute of Standards and Technology*.

conference., W. i. (2020). Sovereignty in cyberspace: Theory and practice (Version 2.0). .

Craigen, D. D.-T. (2014). Defining cybersecurity. TIM Review.

CyberIR@MIT. (2024). Cyber warfare conflict analysis and case studies. MIT Political Science . *MIT Political Science* .

dula, f. (2019). The Federal Democratic Republic of Ethiopia foreign affairs and national security policy and strategy Ministry of Information. .

Eldar Haber& Lev Topor. (2023). Sovereignty cyberspace and the emergence of internet bubbles. .

English, E. (2019). INSA alarmed by increase in cyber attacks, calls for swift actions. .

English, E. (2023). Ethiopia fends off exponential spike in cyber attacks, thwarts over 96 percent of attack.

ENISA. (2024). National cybersecurity strategies guidelines & tools. .

Eyassu, M. (2023). Increasing cyber-attacks target Ethiopia. Abren. .

Eyassu, M. (2023). Increasing cyber-attacks target Ethiopia. Abren. .

Fentaw, M. (2024). The invisible battlefield: Analyzing cybersecurity threats and their implications on Ethiopian national security (2013-2023.

FHI, 3. (2013). Qualitative research methods: A data collector's field guide.

Fortinet. (2023). Top 5 most notorious attacks in the history of cyber warfare. .

GAO., U. (2023). The U.S. now has a national cybersecurity strategy, but is it as strong as it could be? .

GAO., U. (2024). What are the biggest challenges to federal cybersecurity? (High Risk Update). .

Getahun, G. (2022). Cyberattacks in Ethiopia: Reason and consequences. The Reporter Ethiopia.

Getaneh, T. (2018). Cyber security practices and challenges at selected critical infrastructures in Ethiopia: Towards tailoring cyber security framework.

Goel, S. (2011). Cyberwarfare. Communications of the ACM, 54(8). pp. 132–140.

Gracy, M. (2023). How to implement risk management framework (quick guide). Sprinto. .

Gracy, M. (2024). Top cybersecurity challenges facing organizations today. Sprinto.

Groot, J. d. (2020). What is cyber security? Definition, best practices & examples. *Digital Guardian*.

Group., W. B. (2023). World Bank supports Ethiopia's digital ID project to increase access to services and economic opportunities. World Bank. .

Hailu, H. (2015). The state of cybercrime governance in Ethiopia. ResearchGate.

Hayes, A. (2021). Sovereign risk: Definition, types, history, examples. Investopedia.

Helal, M. (2024). Common African position on the application of international law to the use of information and communication technologies in cyberspace, and all associated Communiqués adopted by the Peace and Security Council of the African Union. .

IBM. (2023). Defination of cybersecurity? , What is cybersecurity ? .

IIENSTITU. (2024). Risk management theory explained.

Imperva. (2023). What is cyber warfare | Types, examples & mitigation. Learning Center.

Kaspersky. (2023). What is cyber security? .

Khalid, L. A., Al-Tae, J., Hameeda, A., & Al-Taee, A. . (2020). Relationship of cybersecurity and the national security of the country: Iraq case study. .

Khanna, P. (2018). State sovereignty and self-defence in cyberspace. BRICS Law Journal, 5(4). pp. 139–154.

Khatri, M. (2023). How cyber attacks affect individuals: Understanding the personal impact of digital threats. .

Kore, K. (2019). The impact of social media marketing on consumer behavior .

Kranz, J. & Haeussinger, F. . (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. ResearchGate. .

Krepinevich, A. F. (2012). Cyber warfare: A "nuclear option?". Center for Strategic and Budgetary Assessments. .

LeCompte, M. D., & Schensul, J. J. . (2010). Designing and conducting ethnographic research (Vol. 1). Rowman Altamira. .

Markos, Y. (2022). Cyber security challenges that affects Ethiopia's national security. Social Science Research Network.

Marzagora, S. (2022). Political thought and the struggle for sovereignty in Ethiopian-Japanese relations (1927–1936). .

Melaku, H. M. (2022). Investigating potential vulnerability of critical infrastructure and way forward -- recommendations to enhance security and resilience. Research Square. .

Monitor, E. (2023). In 12 months, INSA foils over 6,700 cyberattacks on Ethiopia.

Munawer, Q. (2023). Egyptian cyberattack on Ethiopian security agency website and some other. The Eastern Herald.

Mustafa, N. (2021). Ethiopia: Cyber-attack targets GERD 2nd filling. Sada Elbalad. .

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). An introduction to information security.

NIST. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. .

Olaoye, G. O., & Adedokun, D. (2023). Digital privacy and security in the age of information and communication technology. ResearchGate.

Posey, B. (2024). Risk management framework (RMF). CIO. .

Prodaft. (2023). Public & private collaboration in the field of cybersecurity. .

Reader, C. (2024). Cyberspace: A new threat to the sovereignty of the state. .

Reqiq. (2024). A daunting digital frontier: The state of cybersecurity in Ethiopia. .

Risk, A. (2024). Cyber security within research and development (R&D) environments.

Robinson, M., Jones, K., & Janicke, H. (2014). Cyber warfare: Issues and challenges. Computers & Security, 49. pp. 70–94. .

Safecore. (2024). Safecore. (2024, January 8). La cyber security nel settore Governativo lo scenario, i rischi e le sfide future.

Shea, S., & Gillis, A. S. . (2024). Defination of Cybersecurit.

Shea, S., Gillis, A. S., & Clark, C. (2023). What is cybersecurity? Security.

Sheldon, J. B. (2010). CyberWar | Cybersecurity, cyberattacks & defense strategies. Encyclopedia Britannica. .

Sibanda, M. (2024). Ethiopia is African country most prone to cyber attacks. ITWeb Africa. .

Slonopas, A. (2024). What is cyber warfare? Various strategies for preventing it. American Public University. .

Sreekumar, D. (2023). What is research methodology? Definition, types, and examples. Paperpal Blog. .

Srivastav, A. K. (2024). Research methodology.

Suganya, K. (2022). Cybersecurity: Threats and challenges. ResearchGate. .

Teshome, M. (2023). Cyber attacks bombard Ethiopia. Capital Newspaper. .

Tunggal, A. T. (2023). Why is cybersecurity important? .

UNODC. (2021). Defination of Cybercrime.

Xinhua. (2024). Ethiopia foils over 4,550 cyberattacks in 6 months.

Yilma, K. M. (2014). Developments in cybercrime law and practice in Ethiopia. Science Direct, 30(6). pp. 720–735.

Appendixes

Appendix: Interview Questions Prepared for Key Informants

Interview Questions for INSA (Information Network Security Agency)

1. What are the most significant vulnerabilities within Ethiopia's cyber infrastructure today?
2. How do these vulnerabilities pose risks to national sovereignty and security?
3. What proactive measures is INSA implementing to mitigate these vulnerabilities?
4. What types of cyberattacks are most frequently encountered in Ethiopia?
5. How have these attacks impacted private companies, government systems, and critical infrastructure?
6. Which sectors are most often targeted, and what might be the reasons?
7. How do Ethiopia's current cybersecurity policies and regulations compare to international standards?
8. What are the main gaps or areas needing improvement in these policies?
9. How does INSA leverage international partnerships to improve Ethiopia's cybersecurity capabilities?
10. What challenges and benefits have arisen from these international partnerships?
11. How does INSA evaluate the skills and abilities of its cybersecurity professionals?
12. How does INSA ensure continuous professional development for its staff?
13. What specific protocols does INSA follow when a cyberattack is detected?
14. How effective are these measures in preventing and mitigating the impact of cyber incidents?
15. What technologies and tools does INSA employ in its cybersecurity efforts?
16. How does INSA collaborate with private companies and other stakeholders on cybersecurity initiatives?
17. What challenges does INSA face in fostering these collaborations?
18. What steps can be taken to improve partnerships and enhance national cybersecurity resilience?

Interview Questions for the Ministry of Foreign Affairs of Ethiopia

1. How does the Ethiopian government evaluate the vulnerabilities in its cyberspace, and what risks do these pose to national sovereignty?

2. Can you discuss specific incidents that have highlighted these vulnerabilities?

3. What types of cyberattacks are most common in Ethiopia, and how do they affect private companies, government systems, and critical infrastructure?

4. Can you provide examples of significant cyber incidents and their impact?

5. How do Ethiopia's cybersecurity policies and regulations compare to international best practices?

6. What are the main strengths and gaps in the current cybersecurity framework?

7. How does Ethiopia leverage international partnerships to enhance its cybersecurity capabilities?

8. What challenges and benefits have arisen from these international partnerships?

9. How does the Ministry of Foreign Affairs evaluate and support the skills and training of Ethiopian cybersecurity professionals?

10. What initiatives are in place to enhance the capabilities of those responsible for cybersecurity?

11. What protocols are in place for international cooperation during a cyber-crisis?

12. How does the Ministry facilitate information sharing and joint efforts in combating cyber threats?

13. How does the Ministry of Foreign Affairs coordinate with other government agencies like INSA on cybersecurity matters?

14. What mechanisms are in place for inter-agency collaboration on cyber defense?

15. How effective are these collaborations in strengthening Ethiopia's overall cybersecurity posture?

Interview Questions for the Ethiopian Communication Authority

1. What are the most significant vulnerabilities within the telecommunications sector's cyber infrastructure today?

2. How do these vulnerabilities pose risks to national sovereignty and security?

3. What proactive measures are telecommunication companies implementing to mitigate these vulnerabilities?

4. What types of cyberattacks are most frequently encountered by telecommunication companies in Ethiopia?

5. How have these attacks impacted private companies, government systems, and critical infrastructure?

6. Can you provide examples of significant cyber incidents in the telecommunications sector and their impact?

7. How do Ethiopian telecommunications companies ensure their cybersecurity measures align with international standards?

8. What are the main strengths and gaps in the current cybersecurity framework for the telecommunications sector?

9. How do telecommunications companies leverage international partnerships to enhance their cybersecurity capabilities?

10. What challenges and benefits have arisen from these international partnerships?

11. How do telecommunications companies evaluate the skills and abilities of their cybersecurity professionals?

12. How do telecommunications companies ensure continuous professional development for their cybersecurity workforce?

13. What specific protocols do telecommunication companies follow when a cyberattack is detected?

14. How effective are these measures in preventing and mitigating the impact of cyber incidents?

15. What technologies and tools do telecommunications companies employ in their cybersecurity efforts?

16. How do telecommunications companies collaborate with government agencies like INSA on cybersecurity initiatives?

17. What challenges do telecommunication companies face in fostering these collaborations?

18. How can these partnerships be improved to better protect national interests?

Interview Questions for the Financial Intelligence Service –Ethiopia

1. What are the most significant cyber vulnerabilities facing the financial intelligence today?

2. How do these vulnerabilities pose risks to national sovereignty and the stability of the financial sector?

3. What proactive measures is the institution implementing to mitigate these vulnerabilities?

4. What types of cyberattacks are most frequently encountered by the financial institutions in Ethiopia?

5. How have these attacks impacted the operations of financial institutions and the overall financial system?

6. Can you provide examples of significant cyber incidents in the financial sector and their impact?

7. How does the financial intelligence ensure its cybersecurity measures align with international standards?

8. What are the main strengths and gaps in the current cybersecurity framework for the financial sector?

9. How effective have these measures been in addressing cyber threats?

10. How does the institution leverage international partnerships to enhance its cybersecurity capabilities?

11. What challenges and benefits have arisen from these international partnerships?

12. How does your institution evaluate the skills and abilities of its cybersecurity professionals?

13. How does the institution ensure continuous professional development for its cybersecurity workforce?

14. What specific protocols follow when a cyberattack is detected?

15. How effective are these measures in preventing and mitigating the impact of cyber incidents?

16. What technologies and tools does the institution employ in its cybersecurity efforts?

17. How does the institution collaborate with government agencies like INSA on cybersecurity initiatives?

18. How can these partnerships be improved to better protect national interests?

Interviewees

Interviewees

Table 1: List of People Interviewed/ Key Informants

Interviewee	Date of Interview	Position	Institution
Hibamo Ayalew	Sep 17, 2024	International Relation officer	MOFA
Anonymous	Sep 17, 2024	Anonymous	MOFA
Abdu Mekonnen	Sep 10, 2024	Investigation and Development unit, Cyber Diplomacy and Political affair division officer	INSA
Anonymous	Sept 10, 2024	Anonymous	INSA
Natnael Tadesse	Sept 25, 2024	Head of Infrastructure security division	ECA
Taddese Getachew	Sep 2, 2024	Internet resource management desk officer	ECA
Mulgeta Temesgen	Sep 2, 2024	Supervision and compliance Directorate director	Financial Intelligence Service-Ethiopia.
Anonymous	Sep 2, 2024	Anonymous	Financial Intelligence Service-Ethiopia.