ADDIS ABABA UNIVERSITY

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING (SITE)

ADDIS ABABA INSTITUTE OF TECHNOLOGY (AAiT)

COLLABORATIVE CYBER THREAT INFORMATION SHARING FRAMEWORK FOR COLLECTIVE CYBER DEFENSE IN ETHIOPIA

BY

MIHIRETU DESALEGN

OCTOBER 2024

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING (SITE)

ADDIS ABABA INSTITUTE OF TECHNOLOGY (AAiT)

COLLABORATIVE CYBER THREAT INFORMATION SHARING FRAMEWORK FOR COLLECTIVE CYBER DEFENSE IN ETHIOPIA

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Cyber Security (Cyber Governance and Management Specialization)

BY: MIHIRETU DESALEGN

ADVISOR: HENOCk MULUGETA (Ph.D.)

OCTOBER 2024

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING (SITE)

ADDIS ABABA INSTITUTE OF TECHNOLOGY (AAiT)

COLLABORATIVE CYBER THREAT INFORMATION SHARING FRAMEWORK FOR COLLECTIVE CYBER DEFENSE IN ETHIOPIA

BY: MIHIRETU DESALEGN

Name and signature of Members of the Examining Board

Henock Mulugeta (Ph.D.) Advisor	_____ Signature	_____ Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that this thesis entitled "*Collaborative Cyber Threat Information Sharing Framework for Collective Cyber Defense in Ethiopia*" is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature_____

Mihiretu Desalegn

This thesis has been submitted for examination with my approval as university advisor

Advisor's signature: _____

Henock Mulugeta (Ph.D.)

Dedication

This work is lovingly dedicated to the memory of my late mother, Genet Hani’a.

Acknowledgements

First and foremost, I would like to express my gratitude to the Almighty GOD for granting me the strength to undertake this research study. I am also thankful to my research advisor, Henock Mulugeta (Ph.D.), for his support and insightful guidance throughout the course of my research. I would like to express my heartfelt gratitude to all the participants involved in this research, particularly those from INSA, EthioTelecom, MiNT, CBE and Wegagen Bank, for your generous cooperation and valuable contributions during the data collection phase. I am also deeply grateful to my friend, Yafet Ashebir, for his kind support and encouragement.

This study would not have been possible without the support of my father, Ato Desalegn Degaga, and my beloved wife, W/o Serkalem Bekele. My heartfelt thanks go to them for their constant encouragement and unwavering support.

Mihiretu Desalegn
October 2024
Addis Ababa, Ethiopia

Abstract

Nowadays, the rapid development of information technology and digitalization has posed a significant challenge to organizations by expanding the attack surface for sophisticated cyber threats. An ordinary security solution by organizations such as end point detection systems, intrusion detection systems, and security information and event management systems are no longer sufficient to address the complexity of these cyber threats. Collaborative approaches for collective cyber defense through sharing threat information is crucial for organizations to proactively defend against the increasing number and complexity of security incidents in the rapidly evolving cyber threat landscape. To improve the current poor culture of collaboration in threat information sharing among stakeholders in Ethiopia, this research proposes an innovative national collaborative threat information sharing framework. This framework includes three essential components: (1) a collaboration structure employing a hybrid CTI (cyber threat information) sharing model that integrates both peer to peer and hub and spoke models to optimize information sharing among stakeholders; (2) a collaboration process inspired by the intelligence lifecycle and aligned with the NIST (National Institute of Standards and Technology) Cybersecurity Framework for efficient threat information sharing; and (3) a collaboration governance component addressing key CTI sharing governance concerns, including legal and regulatory compliance, privacy and security protocols, partnership strategies, training and awareness initiatives, and trust-building measures. This framework is developed with the specific context and legal landscape of Ethiopia, with the aim of ensuring the effectiveness of CTI sharing.

Key words: cyber security; cyber threat; cyber threat information sharing; framework; indicators of compromise

Table of Contents

Declaration ... iii

Dedication ... iv

Acknowledgements ... v

Abstract ... vi

Abbreviations and Acronyms ... xii

CHAPTER ONE ... 1

INTRODUCTION ... 1

1.1. Background Information ... 1

1.2. Statement of the Problem ... 2

1.3. Research Questions ... 3

1.4. Objective of the Study ... 3

1.4.1. General Objective ... 3

1.4.2. Specific Objective ... 3

1.5. Contribution of the Study ... 4

1.6. Scope/Delimitation ... 4

1.7. Structure of the Document ... 5

CHAPTER TWO ... 6

LITERATURE REVIEW AND RELATED WORKS ... 6

2.1. Literature Review ... 6

2.1.1. Cyber Threats ... 6

2.1.2. Cyber Threat Intelligence ... 8

2.1.3. The Intelligence lifecycle ... 10

2.1.4. Cyber Threat Information Sharing ... 12

2.1.5. Cyber Threat Information Sharing Standards and Protocols ... 13

2.1.6. CTI Sharing Models ... 14

2.1.7. CTI Sharing Frameworks and Platforms ... 16

2.1.8. International CTI Sharing Best Practices ... 19

2.2. Related Works ... 22

CHAPTER THREE ... 28

RESEARCH DESIGN AND METHODOLOGY 28
3.1. Overview 28
3.2. Literature Review 28
3.3. Research Design 28
3.4. Data Collection Methods 29
3.5. Data Source 29
3.6. Validity and Reliability 29
3.7. Ethical Consideration 30
3.8. Data Analysis 31
3.9. Chapter Summary 31
CHAPTER FOUR 33
DATA PRESENTATION ANALYSIS AND DISCUSSION 33
4.1. Introduction 33
4.2. Respondents Information 33
4.3. Interview Analysis 33
4.3.1. Current Practices and Methods 34
4.3.2. Challenges on Cyber Threat Information Sharing 36
4.3.3. Awareness and Training Programs 38
4.3.4. Legal and Regulatory Landscape 39
4.3.5. Regulatory Role and Collaborations 40
4.3.6. Recommendations for Enhancing Collaboration 41
4.4. Finding and Discussion 41
4.5. Summary of Findings 46
4.6. Chapter Summary 47
CHAPTER FIVE 48
COLLABORATIVE NATIONAL CYBER THREAT INFORMATION SHARING FRAMEWORK 48
5.1. Introduction 48
5.2. Framework Considerations 48
5.3. Mapping NIST SCF 50
5.4. The Framework Components 52
5.4.1. The Collaboration Structure 53

5.4.2. The Collaboration Process 55
5.4.3. The Collaboration Governance 60
5.5. Validation 65
5.5.1. Participants Selection 66
5.5.2. Evaluation Criteria and Results 66
CHAPTER SIX 68
CONCLUSION AND RECOMMENDATIONS 68
6.1. Conclusion and Recommendations 68
6.2. Limitation and Future Work 69
REFERENCES 71
APPENDICES 77

Tables

Table 1 Traffic Light Protocol [35] 14
Table 2: Comparing CTI Sharing Platforms/Frameworks 19
Table 3: Countries CTI sharing experience 22
Table 4: Summary of Related Works 26
Table 5 Summary of findings, includes thematic areas and codes. 47
Table 6: Comparing literatures adopted the intelligence cycle 57
Table 7: Roles and Responsibilities 64
Table 8: Key performance indicators of collaborative CTI sharing 65
Table 9: Mapped NST CSF Subcategories for the proposed framework 84
Table 10: Subcategories mapped for the collaboration process 87
Table 11: NIST CSF subcategories mapped for the collaboration governance layer 88

Figures

Figure 1: Types of Threat Intelligence [26]. 9
Figure 2: The Intelligence Lifecycle [30]. 11
Figure 3: Peer-to-Peer Sharing Model 15
Figure 4: Hub-and-Spoke Sharing Model 16
Figure 5: Hybrid Sharing Model 16
Figure 6: NIST Cyber Security Framework [54] 18
Figure 7: The Mapped Subcategories form the NIST SCF 51
Figure 8: The Collaborative CTI Sharing Framework 53
Figure 9: The Collaboration Structure 55
Figure 10: The Collaboration Process 60
Figure 11: The Collaboration Governance 61

Abbreviations and Acronyms

ACSC: Australian Cyber Security Center

APT: Advanced persistent threat

A-ISAC: Aviation Information Sharing and Analysis Center

CAPEC: Common Attack Pattern Enumeration and Classification

CSA: Cyber Security Agency

CSIRT: Computer Security Incident Response Team

CSF: Cyber Security Framework

CII: Critical Information Infrastructure

CI: Critical Infrastructure

CISA: Cybersecurity and Infrastructure Agency

CTI: Cyber Threat Intelligence/ Information

CyBox: Cyber Observable Experssion

CMCSRS: Critical Mass Cyber Security Requirement Standard

DDoS: Distributed denial-of-service

ENISA: European Network and Information Security Agency

E-ISAC: Electricity Information Sharing and Analysis Center

FS-ISAC: Financial Services Information Sharing and Analysis Center

IDS: Intrusion Detection System

INSA: Information Network Security Administration

IoC: Indicators of Compromise

IODEF: Incident Object Description Exchange Format

IPS: Intrusion Prevention System

ISAC: Information Sharing and Analysis Center

ITU: International Telecommunication Union

KPI: Key Performance Indicator

MISP: Malware Information Sharing Platform

NCSC: National Cyber Security Centre

NIST: National Institute of Standards and Technology

OpenIOC: Open Incident of Compromise

RID: Real-time Inter-Network Defense

STIX: Structured Threat Information eXpression

SEIM: Security Event and Incident Management

TTPs: tactics, techniques and procedures

TAXXI: Trusted Automated eXchange of Indicator Information

TI: Threat Intelligence

UTM: Unified Threat Management

USD: United States Dollar

VERIS: Vocabulary for Event Recording and Incident Sharing

WAF: Web Application Firewall

CHAPTER ONE

INTRODUCTION

This chapter provides the necessary context for the research, describing the problem statement, associated research questions, objectives of the study, purpose of the study, and scope. The structure of the thesis is also explained in this section.

1.1. Background Information

The rapid technological progress in the cyberspace has created globally interconnected networks that bridges borders by enabling seamless information sharing and collaboration from every corner of the world with click on button. The technological innovations with the emerging technologies facilitated efficient data collection, storing and sharing, and these advancements also introduced new vulnerabilities and cyber security threats that can target countries, institutions, and individuals [1] [2].

The total average cost of data breach worldwide in 2024 was 4.88 million USD, according to the IBM cost of data breach report [3]. This result is a 10% increase from the 2023 report which is USD 4.45 million. Cyber security attacks continued to increase in terms of attack vectors, number, and their impact as indicated by the ENISA threat landscape report [4]. As the paper [5] indicated, about 38% of African population uses internet, which is expected to grow in the coming years. This poses a significant threat to the future, with the rise of malicious actors exploit increasing vulnerabilities. Kaspersky reported that Ethiopia, along with other African countries such as South Africa, Kenya, Egypt, Nigeria, and Rwanda, encountered the highest number of phishing attempts in 2020, amount to a total of 2 million [5]. During a discussion held on the third National Cyber Security month, the Information Network Security Administration (INSA) revealed that over 1600 attacks on different organizations were made in the first quarter of the 2015 Ethiopian fiscal year alone. At the end of the 2014 Ethiopian fiscal year, INSA noticed an over tenfold increase in cyber-attacks, and 791 in 2011 increased to 8,845 [6].

Cyber threat information sharing has become an increasingly important realm of cybersecurity [7]. As cyber threats grow more advanced, organizations must be well prepared to counter them. This

is particularly important for developing nations, where the availability and quality of CTI sharing are often less than ideal [5]. Given the transnational and rapidly evolving nature of cybercrime, effective counter-cybercrime strategies that require coordinated, rapid responses facilitated by robust threat intelligence sharing is required in Africa [5]. As research indicated [8][9], Ethiopia is among one of such countries that need to improve their threat intelligence-sharing capabilities. This paper explores the current state of threat intelligence sharing in Ethiopia, identifies challenges of sharing CTI in Ethiopia, and proposes threat intelligence sharing framework that offers recommendations and guidelines for improving the current cyber defense posture of the country.

1.2. Statement of the Problem

Cyber threat information is an information that can be used by organizations to identify, assess, monitor, and respond to cyber threats. It includes system compromise indicators, threat actor tactics, techniques and procedures (TTPs), security incident alert information, recommendations to detect, contain, or prevent attacks, and incident analysis results. Collaborative cyber threat information sharing across organizations is crucial for improving their security posture, reducing cyber threat risks, building cyber resiliency, and strengthening the threat intelligence capability that reduces effort duplication with proactive incident detection and response to increased situational awareness.

According to previous studies regarding cyber security in Ethiopia, critical infrastructure organizations face a lack of expertise, inadequate technology, and poor preparedness to detect, prevent, and respond to different forms of cyber-attack. Also, research shows that most critical infrastructure organizations in Ethiopia do not have an organizational structure regarding cyber security governance, and almost all cyber-attack incidents were not reported to the concerned stakeholders. The current state regarding collaboration in sharing threat information is poor, even in organizations that have implemented cybersecurity administration structures. The practice of threat information sharing between organizations and reporting potential threats to relevant regulators is not satisfactory. Currently, there is no regulatory framework, or platform for cyber threat information sharing for organizations in Ethiopia.

The main purpose of this study is to propose a collaborative national cyber threat information sharing framework by assessing the current state of stakeholder collaboration in the sharing of

cyber threat intelligence in Ethiopia. This study aims to identify gaps and challenges in CTI information sharing, factors that hinder stakeholder collaboration in threat information sharing, and recommendations improve stakeholders' cooperation for more effective CTI information sharing. This study seeks to determine the processes that can be implemented or modified to ensure a greater degree of success in CTI sharing between stakeholders and to increase the efficiency and effectiveness of responses to cyber threats. The research will also explore the status of regulatory bodies in relation to cyber threat intelligence sharing, proposing cyber threat information exchange framework, endorsing international best practices and guidelines for distributing cyber threat data, examining legal, privacy, and compliance considerations, and trust in the sharing of cyber threat data among stakeholders in Ethiopia. Finally, it provides recommendations on specific measures necessary for increasing stakeholder collaboration that will help enhance the cyber security posture of organizations by effectively utilizing CTI information sharing in Ethiopia.

1.3. Research Questions

The goals of this study are formulated in the following main research questions:

- What are the current practices, processes, and challenges of collaborative cyber threat intelligence sharing among stakeholders in Ethiopia?
- What is the role of regulatory bodies in establishing coordinated cyber threat intelligence sharing involving multiple institutions or stakeholders?
- What measures and recommendations should be applied to improve stakeholder collaboration between organizations to effectively share cyber threat intelligence information?

1.4. Objective of the Study

1.4.1. General Objective

The main objective of this study is to develop a collaborative national cyber threat information (CTI) sharing framework for collective cyber defense in Ethiopia.

1.4.2. Specific Objective

To achieve the stated general objective, the following specific objectives are framed.

- To assess the current practices, processes, and challenges of collaborative cyber threat intelligence information sharing among regulatory bodies and stakeholders in Ethiopia.
- To propose a framework for collaborative cyber threat information with recommendations that should be applied to improve stakeholder collaboration to effectively share CTI information in Ethiopia.

1.5. Contribution of the Study

This study contributes to existing efforts by determining the difficulties that hinder stakeholder collaboration for threat information sharing in Ethiopia. The research conducted can show organizations how they can collaborate to exchange cyber threat intelligence information and suggest the most effective approaches to improve collaboration in relation to threat data exchange among regulatory bodies, governmental institutions, private organizations, and the public. This research will provide a valuable foundation for regulatory bodies and policy makers to develop policies and regulation regarding CTI sharing in Ethiopia. And it will assist regulatory bodies to enforce and promote effective and efficient CTI sharing among sharing community. This study provides a comprehensive breakdown of the current state of collaborative cyber threat intelligence sharing, reveal existing challenges, establish best practices, and offer suggestions on how to address these issues. This study also proposes a comprehensive framework that addresses the governance and practice of threat information sharing. This framework will improve the current threat sharing practices, privacy and security issues, legal and regulatory compliance concerns, and risk management for cyber threat information sharing among stakeholders. This research will pave the way for more comprehensive future researches in the field of CTI sharing by filling the current information gap on cyber threat information sharing in Ethiopia.

1.6. Scope/Delimitation

This study explores the extent to which stakeholders can collaborate in cyber threat intelligence information sharing in Ethiopia. It focuses specifically on examining existing challenges, approaches, and practices related to threat information sharing for collaborative security. The study also proposes a framework for collaborative CTI information sharing among stakeholders to maintain strong situational awareness and enhance cybersecurity posture. This study limited to cyber threat intelligence information sharing collaboration among stakeholders, it does not focus

on concepts such as vulnerabilities assessment and incident monitoring. It does not involve in developing threat intelligence platforms or tools, rather it focuses on adopting and embedding existing platforms and tools within the proposed framework.

1.7. Structure of the Document

This paper consists of five chapters. The initial chapter serves as an introduction, which provides the background of the study, a statement of the research problem, research questions, objectives of the research, significance of the study, and scope with limitations of the research.

In the second chapter, the literature review looks at both the conceptual elements and contextual knowledge of cyber threats and cyber threat intelligence, as well as examining how cyber threat intelligence is shared and the standards established for this intelligence exchange between organizations. This chapter reviews related research studies concerning incident response and stakeholder collaboration in cyber threat information sharing, nationally, regionally, and globally.

The third chapter examines the research design and methodology used in this study, including the data collection methods, data analysis techniques, and ethical considerations. Chapter Four features the presentation, analysis, and discussion of data. Chapter five presents the conclusion, recommendations, and possible areas for future research.

CHAPTER TWO

LITERATURE REVIEW AND RELATED WORKS

2.1. Literature Review

In this section, we explore the realm of cyber threat intelligence and its associated standards for collaborative CTI sharing across organizations. This section provides a theoretical background for answering the research questions of this study, as well as an overview of the relevant literature.

2.1.1. Cyber Threats

A cyber threat as defined by NIST SP 800-150 [7] "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."

The "Picus Labs" report 2022 [10] and numerous literatures such as [11][12] show that ransomware, phishing, web application and vulnerability exploitation attacks (attacks such as Local File Inclusion, SQL Injection, Cross-Site Scripting and Exploitation of known and Zero-Day vulnerabilities [13][14]), distributed denial of service (DDoS) attacks, insider threats, state-sponsored and Advanced Persistent Threats (APTs) are the most dominant threats to the critical infrastructure institutions.

In the most recently reported quarter of the 2022/23 Fiscal Year, the Information Network Security Administration (INSA) noted that Ethiopia had been subject to more than 1600 attempted cyber-attacks, revealing a heightened period of malicious online activity in the country. The report stated that the rise in technology and lack of awareness regarding cyber security were contributing factors to the rising number of cyberattacks. INSA mentioned that hackers utilize deep fake and social

engineering strategies more often, both inside Ethiopia and all over the world [15]. The following are the most prominent types of cyber threat:

Social Engineering Attacks

Social engineering cybersecurity attacks rely on humans to be successful and use different forms of manipulation activities that trick victims to gain access to sensitive information by exploiting weaknesses in human behavior. Social engineering attacks lure victims to click buttons, open files, or emails, and visit malicious pages. This threat encompasses phishing, spear-phishing, smishing, vishing, fraud, impersonation, and so on [4].

Phishing remains a common type of attack that mainly involves stealing user information, such as login credentials and credit card numbers, by tricking the victim to open a malicious link. After the attacker gains access to a network as a part of a larger attack, such as malware or advanced persistent threat (APT), it can distribute malware inside the network or gain privileged access to sensitive data. Recently, the concept of phishing as a service has become prevalent because skilled developers create a phishing kit that targets attack institutions. Spear phishing is another complex form of phishing that targets specific organizations or individuals. Smishing combines SMS with phishing to gather personal information of a target using SMS messages. Vishing another related social engineering threat uses voice to obtain personal information through the phone [4], [13].

Malware

Malicious software or firmware is intended to perform an unauthorized action with an adverse impact on the confidentiality, integrity, or availability of the system. Malware variants such as Viruses, Trojans, Spyware, Ransomware, Adware/Spamming and Botnets can provide unauthorized access or cause damage to systems [4], [16].

Ransomware

Ransomware is a type of malware that encrypts victim system or data to prevent them from accessing and the attacker terrorizes the victim that it is going to disclose or sell the encrypted data until ransom fee is paid [17]. Recent study by security magazine [18] indicate that there is 1318% increase of ransomware attack in 2021. In 2017, WannaCry ransomware appeared as most damaging malware and spread independently through the networks of unpatched Microsoft

windows SMB Server Remote Code Execution Vulnerability, leaving numerous systems and computers infected 150 counties [19].

Distributed denial of service (DDoS) attacks

Distributed Denial of Service (DDoS) attacks crash a target system by generating flood of traffic from different compromised connected devices. These attacks pose an extensive damage to organizations by interrupting business operations. According to study by [13], there is 93% increase of DDoS attacks on financial institutions between 2018 and 2020, this indicates that applications, daily critical services, systems and operations of financial industry are disrupted by cyber criminals. Also this study showed that DDoS attacks in the financial service industry increased by 110% in the year of 2020 when compared to the previous year.

Insider Threats

Besides other sophisticated cyber-attacks on organizations information and information infrastructures, plenty of cyber security incidents are result of insider threats by former or current staff conducting malicious actions using access to internal systems [20]. According to insider threat report 2020 [21], insiders with privilege to access the organization information resources are more challenging to detect with higher degree of damage and the attacks are becoming more prevalent.

2.1.2. Cyber Threat Intelligence

Threat intelligence is a growing and relatively new area of research in the field of cybersecurity as noted in [22]. The effectiveness of cyber threat intelligence sharing largely depends on the steps and efforts taken to assemble threat information into timely and applicable threat intelligence. Threat intelligence is about gathering and analyzing information regarding potential threats or hazards to an organization's assets to gain insights and create actionable strategies to respond effectively [22]. It encompasses collecting knowledge with accompanying context, mechanisms, indicators, implications, and guidance on how to respond to it, to inform decisions regarding the protection of organization's assets. It involves gathering information from various sources to gain insight into potential threats towards a specific environment [23]. Examples of CTI include

indicators, security alerts, incident reports, threat intelligence and other information about recommended or vulnerable configuration settings for security tools [24].

Based on the aim and consumer of threat intelligence,[25] [26]categorizes cyber threat intelligence in four subdomains: Strategic, Operational, Tactical and Technical threat intelligence. Strategic CTI focuses on providing high level intelligence for decision makers to help organization to develop long term strategies [26]. Operational threat intelligence is about specific upcoming attacks that target an organization and is first used by senior level security personnel, such as incident response heads or security managers [26]. Tactical threat intelligence involves the identification of how threat actors carry out attacks through the collection of information on their tactics, techniques, and procedures (TTPs). Defenders and incident use tactical TI to make sure that their defense, alerting systems and investigations are capable enough to deal with recent attack tactics. If threat intelligence information is about specific attacks on an organization and collected from internal logs, Indicators of Compromise (IoC) and threat actor behaviors, it is technical threat intelligence [26].

Figure 1: Types of Threat Intelligence [26].

An organization can leverage cyber threat intelligence information from internal and external sources [23]. The internal threat intelligence source consists of events that have been observed on the organization's internal network and its hosts such as system logs and events, network events, alerts from boundary devices (IDS/IPS, Firewall, WAF), Alerts from anti-virus systems, staff and etc. Organizations can acquire threat intelligence from external sources, such as data subscriptions or feeds, commonality based on industry or geographic location, from relationships with government and law enforcement and crowdsourced platforms [23], [24].

Cyber threat information comes from many sources, including threat actors, threat indicators, TTPs, security alerts, vulnerabilities and more. Here are the main types of cyber threat information.

- Threat Actors: individuals, groups or organizations behind a cyber attack [7].
- Tactics, techniques, and procedures (TTPs): attack methods used by threat actors [27].
- Indicators of compromise (IOC): includes threat indicators information with potential cyber threat such as IP addresses, malware signatures or hashes, email addresses, domain names associated with attacks [28].
- Vulnerabilities: details on system weaknesses that can be exploited by attackers to gain unauthorized access [24].
- Security alerts and advisories: can be vulnerability notes, security advisories and bulletins that are human readable briefs and technical notifications related to current security issues. Advisories are specific steps to respond to cyber attacks, to mitigate threats, to close vulnerabilities and to recover from incidents. Advisories include software patches, antivirus updates, specific IP to block, and instructions to block malicious activities on the networks [7]
- Cyber threat intelligence reports: include information about specific incidents, indicators, TTPs, threat actors, attack campaigns, and targeted systems and data [7].

2.1.3. The Intelligence lifecycle

The intelligence cycle is a cyclical process that outlines the key steps involved in gathering, processing, and disseminating threat intelligence. This framework is crucial for organizations to effectively foresee, prepare and mitigate potential security threats. While different literatures present intelligence lifecycle in somewhat different ways, the paper [29] represented intelligence

cycle that comprises of five stages, namely the planning and direction stage, the collection stage, processing stage, analysis stage, and dissemination stage [29]. The research [30] groups CTI in six stages as follows. The planning and direction stage deals with the identification of key stakeholders and organizations establish their objectives, priorities, and requirements regarding threat intelligence. The second stage is the collection stage involves collecting CTI data such as IoCs, malware samples, and network traffic logs using identified data sources. Data processing involves structuring and cleaning raw data into a structured format that can be used for analysis. The potential threats, patterns, and trends of processed data are identified in the analysis phase. Threat information sharing with relevant stakeholders is during the dissemination stage. The feedback phase involves the continuous improvement of the CTI lifecycle using feedback collected from various stakeholders to evaluate the effectiveness of threat intelligence for refine and improve future iterations in the lifecycle. The research [31] also adopted the six-phase intelligence cycle as a model for the intelligence process. The study [32] proposes CTI framework adopting the intelligence lifecycle with four components namely, direction and planning, data collection, data analysis and sharing and visualization. The above four literatures [29] [30] [32] [31]shows different researchers adopt the threat intelligence lifecycle and customize it according to their specific scenario.

Figure 2: The Intelligence Lifecycle [30].

2.1.4. Cyber Threat Information Sharing

Organizations have traditionally communicated threat information through informal or ad-hoc methods like phone calls, encrypted emails, and ticketing systems, and more recently, they have utilized portals and blogs [25]. The concept of cyber threat information sharing first started by the US government in the late 1990s that encompasses the sharing of threat information between countries, between governments at all levels, between governments and private enterprises, and among private enterprises [33].

Existing literatures generally agrees on the idea that coordination and collaboration significantly strengthen the ability to mitigate and respond to cyberattacks effectively. These cooperative efforts not only enhance collective understanding and knowledge but also improve the capacity to identify threats, assess future risks, recognize incentives for potential attacks, increase detection rates, optimize cybersecurity investments, and strategize for future investments [34].

The contribution of cyber threat information sharing to organizations includes enhancing their cyber defense capabilities by creating coordinated engagement of concerning stakeholders to defend against evolving cyber threats, provides better situational awareness on the cyber threat landscape that enables timely exchange of vulnerabilities, increases the understanding of a given organization about threat actors including their tactics, techniques, and procedures (TTPs), and improves collaborative incident response that reduces redundant occurrence of same incident among stakeholder organizations[35][36].

Currently there are different organizations such as government and private sectors, nonprofit organizations, local and international entities participate in sharing cyber threat intelligence information. Information Sharing and Analysis Center (ISAC) is one of threat intelligence information sharing within specific industries [37]. It was proposed by the U.S. government in the Presidential Decision Directive-63 (PDD-63), published in 1998 with the aim of enabling critical infrastructure organizations to establish sectoral based organizational structure for threat and vulnerabilities information sharing [37]. ISACs are established to maintain sectoral situational awareness by enabling sectors within specific industry to share trusted and secure cyber threat information among related sectors such as education, energy, aviation, mining, communications, and finance [37]. The role of ISACs is collection, analysis, dissemination of actionable cyber threat

intelligence information and provision of risk mitigation tools to enhance cyber threat resilience of their sector organizations [46], [47].

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is one of most successful and mature ISACs formed to enable timely and secure cyber threat intelligence sharing among financial sector stakeholders. Currently FS-ISAC has members and partners from all over the world. Other sector specific ISACs such as Aviation ISAC (A-ISAC) for aviation-focused information sharing and analysis, Electricity ISAC (E-ISAC) establishes timely, reliable and secure information sharing and analysis within the electricity sector [47].

There are also other cyber threat intelligence information sharing initiatives: ENISA, the European Network and Information Security Agency [42] has proposed an initiative with the aim to avoid duplication of effort of European institutions and Member States by improving threat information exchange. NIST, the National Institute of Standards and Technology has special publication NIST SP 800-150 [7] which provides guidance and best practices that can help organizations to establish and participate in cyber threat information sharing collaborations.

2.1.5. Cyber Threat Information Sharing Standards and Protocols

From the several efforts to standardize the process of cyber threat information sharing the notable ones are STIX (Structured Threat Information eXpression) [43] [44] and TAXII (Trusted Automated eXchange of Indicator Information) [45] [44]. STIX, developed by MITRE Corporation, is a language used to describe cyber threat information in a standardized and structured manner. The STIX specification includes IP addresses and file hashes, along with additional contextual details about threats, such as threat actors, TTPs, exploitation targets, campaigns, and courses of action. Because of this standardization by STIX, organizations or systems can easily understand and utilize the threat information effectively [43] [44]. The MITRE Corporation developed TAXII, a protocol that makes it easier to share cyber threat intelligence (CTI) that is represented in STIX. It specifies formats and procedures for securely exchange threat intelligence, including indicators of compromise (IOCs). Threat information is transported by TAXII, which offers a framework to exchange threat data, while STIX standardizes the structure of threat information.

Other threat information sharing standards include RID (Real-time Inter-Network Defense) [44], OpenIOC (Open Incident of Compromise) [44], CyBox (Cyber Observable Experssion) [44], VERIS (Vocabulary for Event Recording and Incident Sharing) [44], IODEF (incident object description exchange format) [44] and CAPEC (Common Attack Pattern Enumeration and Classification) [44]. However, there are other several standards and protocols that organizations, computer security incident response teams (CSIRTs) and ISACs use based on their specific needs to facilitate the timely sharing of cyber threat intelligence information [46], [53], [54].

The cyber threat intelligence information managed to be shared with the sharing standards such as STIX and TAXII can be given a security classification using Traffic Light Protocol (TLP). The TLP classification is done according to the sensitivity and potential impact that could result from the disclosure of the information. The TLP framework defines the information sensitivity and its impact when disclosed in four levels TLP RED, TLP AMBER, TLP Green and TLP WHITE as depicted in *table 1* [50].

TLP Color	**Threat Level**	**Description**
TLP:RED	CRITICAL	Not for disclosure, restricted to participants only.
TLP:AMBER	HIGH	Limited disclosure, restricted to participants' organizations.
TLP:GREEN	MEDIUM	Limited disclosure, restricted to the community.
TLP:WHITE	LOW	Disclosure is not limited.

Table 1 Traffic Light Protocol [35]

2.1.6. CTI Sharing Models

Stakeholders can engage together to create a CTI sharing collaboration that can operate as either a peer-to-peer, peer-to-hub, or hybrid [51]. In peer-to-peer threat intelligence sharing model all the sharing exchanges takes place between individual entities. The groups that produce information have direct relationship with the consumers [52]. This is more convenient for targeted or classified information sharing between organizations established greater degree of trust with each other [36]. Establishing a trustworthy environment among stakeholders is the challenge associated with this approach [25]. The other sharing model is called the hub-and-spoke model where the central hub is responsible to collect and handle dissemination of information to all the other spokes or stakeholders as needed [52]. This model is preferred to enrich the source data with additional

context, ensure data accuracy by performing validation and sanitization and sanitize the information by de-identifying or anonymizing [36]. The main drawback of this approach it its dependence on the performance of central hub, which exposes the stakeholders to response delays. Since time-sensitive information is usually critical, delays in distribution can reduce the importance of the threat information sharing, and affect the relevance of the information [25]. The hybrid model is when using blended approach by applying both peer-to-peer and hub-and-spoke data sharing as appropriate [51].

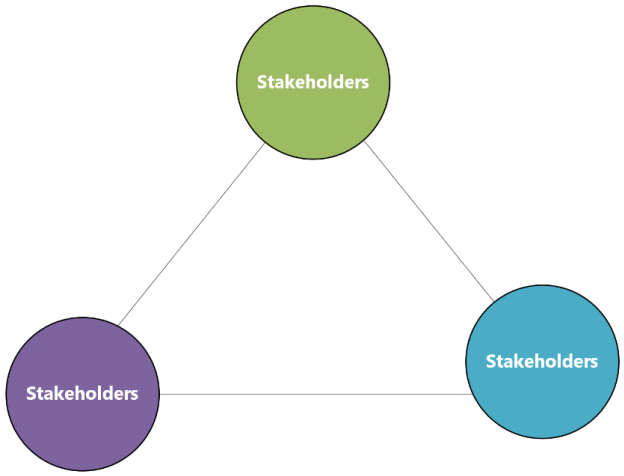

Figure 3: Peer-to-Peer Sharing Model

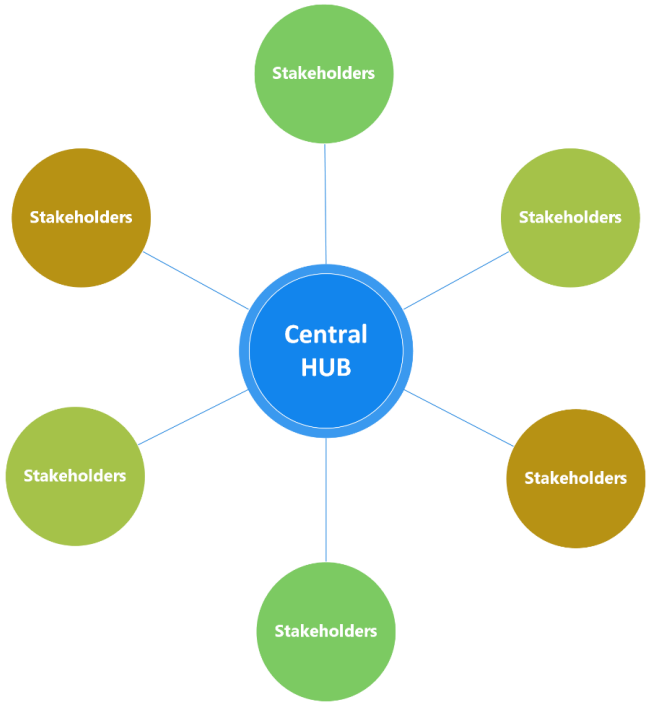

Figure 4: Hub-and-Spoke Sharing Model

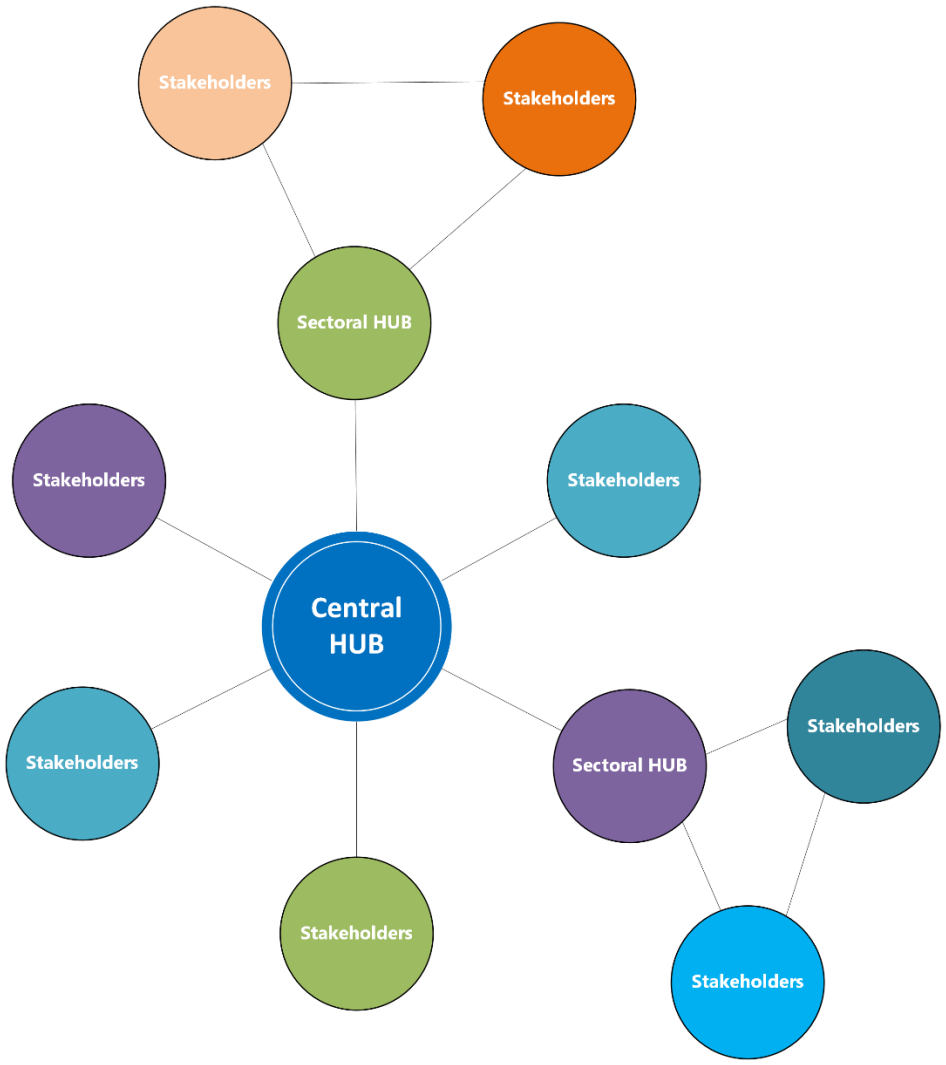

Figure 5: Hybrid Sharing Model

2.1.7. CTI Sharing Frameworks and Platforms

In this section we will explore few of existing platforms, frameworks and best practices for cyber threat intelligence information sharing.

Malware Information Sharing Platform (MISP)

The Malware Information Sharing Platform (MISP) serves as a hub to exchange cyber threat intelligence within trusted groups. Users of this open-source platform can exchange information regarding financial fraud, malware and targeted attack, Indicators of Compromise (IOCs). Because

MISP uses a distributed model, information can be shared in private, closed groups or even made public, regardless of whether it is technical or not [53].

MISP functions as a tool that makes it easier for members of its community to share information. It makes use of data models that contain objects such as "organizations" and their associated "users". The MISP platform offers various options for controlling who sees shared cyber threat information, such as organization, community, public or sharing groups [53].

NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) developed Cybersecurity Framework (CSF) which aims at addressing the cyber security requirements of critical infrastructure organizations [54]. Because of the flexibility and customization this approach offers, organizations may easily integrate the CSF with their current cybersecurity initiatives and risk management procedures [54].

The CSF has five core functions that provide security protocols and best practices to manage the cyber security risk throughout an organization's life cycle. Each function is further divided into 22 categories, representing specific cybersecurity outcomes an organization should strive for. There are 98 subcategories in total, with number of cybersecurity outcomes and controls are defined for each category. These subcategories define more detailed outcomes that can be implemented through a combination of technical and management activities. Each subcategory informative references relevant global standards and best practices, provide practical guidance to achieve the desired outcomes. This ensures the framework remains neutral and adaptable to different contexts [54]. *Figure 5* provides the five functions of the NIST cyber security framework.

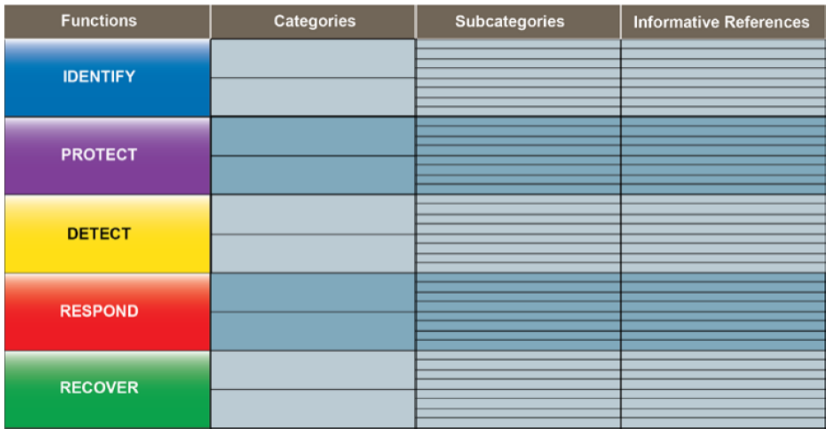

Figure 6: NIST Cyber Security Framework [54]

MANTIS Cyber Intelligence Management Framework

The MANTIS (Model-based Analysis of Threat Intelligence Sources) is an open-source Framework by Siemens that consists of several Django Apps. MANTIS, an analysis platform for storing, authoring and managing cyber threat intelligence information expressed in standards such as STIX, CybOX, IODEF, OpenIOC, etc [55].

Although MANTIS is not a fully developed system, can be used as an threat information repository where received threat intelligence in formats such as STIX/CybOX, OpenIOC, and IODEF can be imported for effective filtering and searching of information. Thus, MANTIS can be used as a database for storing all received information and the information that is self-generated using any of the supported standards [56].

Soltra Edge

Soltra Edge emerged as a result from an initiative by Financial Services Information Sharing and Analysis Center (FS-ISAC) to create a common platform to share threat information such as indicators of compromise. Though it started to facilitate sharing of threat information between the member organizations within the financial sector, it can also be deployed for other sharing groups [56]. Avalanche is the name of its free version, currently it developed into a quasi-commercial product supported by Soltra. It is integrated with threat sharing industry standards such as STIX and TAXII [25].

Critical Infrastructure Threat Information Sharing Framework

Critical infrastructure threat information sharing framework is a national cyber threat information sharing framework proposed for the U.S. Government [57]. The framework is designed to facilitate the sharing of threat intelligence among federal, state, corporate, and local agencies. The framework defined the existing entities that take part in the critical infrastructure threat information sharing process and proposes a process to share threat information. The key hubs to share threat information at the federal and regional levels are identified under this framework. The National Infrastructure Coordinating Center (NICC), fusion centers, Information Sharing and Analysis Centers (ISACs), and Information Sharing and Analysis Organizations (ISAOs) are among the current threat information sharing units that are identified [57].

ICARO (Spain)

The Spanish national cybersecurity institute created the ICARO platform to facilitate the exchange of cyberthreats [42]. The tool is built on the Malware Information Sharing Platform (MISP) [58], which allows it to share information about cyber threats, including indicators of compromises across private and public institutions. To join and share threat data with others, companies must sign threat sharing agreements [42].

Comparing Existing CTI Sharing Platforms/ Frameworks

Framework/ Platform	**Description**	**Supported Standards and Integration Capability**	**Limitation**
NIST CSF	Developed to address the cybersecurity needs of critical infrastructure	Recommends use of standards, Integration	Not specifically designed for CTI sharing but only depicts recommendations and standards for CTI sharing
ICARO (Spain)	CTI Sharing Platform	MISP (MISP supports STIX, CybOX, TAXII) [22]	Specifically developed for Spain
Critical infrastructure threat information-sharing framework	CTI Sharing Framework	Well known Standards/Platforms such as MISP, STIX, CybOX, TAXII	Specifically developed for USA
Soltra Edge	CTI Sharing Platform	STIX, TAXII	• Specific to the Financial Sector • It is a platform that can be integrated to Threat sharing Frameworks
MANTIS Cyber Intelligence Management Framework	CTI Sharing Platform	STIX, CybOX, IODEF, OpenIOC	It is a platform that can be integrated to Threat sharing Frameworks

Table 2: Comparing CTI Sharing Platforms/Frameworks

2.1.8. International CTI Sharing Best Practices

The study [49] shows that while various standards exist for sharing cyber threat information, there's no single, universally adopted set of standards by organizations and by computer security incident response teams (CSIRTs) at organizational, sectoral, national, and international levels. This lack of standardization hinders effective communication and collaboration between organizations and

sectors at national and international levels. To improve cybersecurity preparedness, harmonized adoption of threat information sharing standards is necessary so that all stakeholders can speak the same language and can work together seamlessly.

A case study in Saudi Arabia [59] finds that the absence of a centralized system for exchanging threat information hinders effective threat information sharing. This aligns with research findings from Europe [60] there is lack of effective tools to support the collaborative operation from the national cyber security centers. The study on united states threat intelligence frameworks [37] points out challenges in coordinated threat sharing such as classification of information, trust, interoperability, preserving privacy. A 2020 World Economic Forum report [61] on cyber information sharing found that only few of African countries have formal cybersecurity strategies in place. The report revealed that just eight countries have a national cybersecurity strategy, and only 13 have a government-run computer emergency response team (CERT), which are key to setting up national information sharing programs.

The international standards have created guidelines and suggestions for collaborative sharing of threat information. Notably, entities like the NIST Special Publication 800-150 (Guide to Cyber Threat Information Sharing) [7] , ITU guide on developing a national cyber security strategy guide 2021[62], the ISO/IEC 27010:2015 Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications [63] and ENISA National Cyber Security Strategies Good Practice Guide[64] have put forward mechanisms and guidance for stakeholders sharing threat information, often involving central coordinating bodies such as national or industry-specific cybersecurity centers. To discuss more:

- The ITU guide on developing a national cyber security strategy guide 2021 recommends establishing a domestic cyber security legal framework that provide guidance on how to deal with common regulatory approaches that concern cross-sectoral exchange of information and intelligence sharing mechanisms, and public-private cooperation [62].
- The NIST Special Publication 800-150 (Guide to Cyber Threat Information Sharing) [7] provides guidance to help organizations exchange cyber threat information. This publication focuses on the importance of sharing threat information such as indicator of compromises, TTPs, security alerts, and threat intelligence reports. It emphasizes that organizations should follow rules governing the exchange of threat information. It also

emphasizes the importance of building trust among sharing communities, standardized data formats and transport protocols to achieve interoperability, and handle sensitive information securely.

- The ENISA National Cyber Security Strategies Good Practice Guide [64] recommends establishing trusted information-sharing mechanisms among private and public stakeholders to better understand and respond to the constantly changing threat landscape. This guide also recommends setting a clear cyber governance structure that defines the roles, responsibilities and accountability of all relevant stakeholders for successful cyber security strategies.
- ENISA [42] has proposed an initiative of forming sector-based ISACS with the aim to avoid duplication of effort of European institutions and member States by improving threat information exchange. It emphasizes the stakeholders to invest in building trust when forming ISAC institutions and the participants the Traffic Light Protocol (TLP) for information sharing.

Comparing Cyber Threat Sharing Experience of Countries

Different countries follow different approaches for threat information sharing according to the specific context of each country. Successful national threat sharing frameworks often have unique features and approaches designed to their specific contexts such as political, economic, technological, and cultural context of each country to ensure the framework relevant, effective, actionable, and sustainable. As clearly indicated on [57] the cyber threat information sharing approach followed in the US is decentralized network of formal and informal channels through which government entities and the private sector share information. Whereas UK's national cybersecurity strategy [65] emphasizes the role of the National Cyber Security Centre (NCSC) as a central coordinating body for cybersecurity efforts by following more centralized approach in which the government takes the leading role. As the study by [66] indicates countries form specific organization responsible for threat information sharing and uses its own approach and platform to improve the effectiveness and efficiency of cyber threat information sharing. *Table 3* shows the cyber threat sharing experiences of few countries.

Country	Institution	The CTI Sharing Framework/ Platform
Spain	Spanish National Cybersecurity Institute	ICARO Platform
Australia	Australian Cyber Security Center (ACSC)	TISN platform and supported by JCSC
USA	Cybersecurity and Infrastructure Agency (CISA)	NICC Platform, CISA Gateway
Singapore	Cyber Security Agency (CSA)	OT-ISAC Platform
UK	National Cyber Security Center (NCSC)	CISP Collaboration Tools

Table 3: Countries CTI sharing experience

2.2. Related Works

This section provides an overview of the related studies on cyber threat intelligence sharing between organizations conducted globally, as well as reviews of recent and relevant works in Ethiopia.

Cyber resilience and collective knowledge of recent complex and dynamic cyber-attacks on critical information infrastructure of organizations can be improved by sharing cyber threat intelligence information across organizations. An organization can become better prepared to new cyber-attacks and TTPs that haven't encountered it before by acquiring threat intelligence information from another organization or threat source.

Survey research [67] to assess cyber security practices and challenges on selected three critical infrastructure organizations, tries to tailor framework to enable critical infrastructures respond for cyber threats that obligates the cyber security units of critical infrastructures and INSA together to create bags (storages) of cyber threats proactively. The tailored framework does not show how cyber security units of critical infrastructures collaborate with each other in sharing cyber security threats. It doesn't define the governance of the constructed threat bags, legal issues, privacy issues, sanitization of threat data, international standards and protocols for sharing threat information among organizations.

The paper [8] done on assessing information security incident management practices within Ethiopian banking sector taking one bank as a case study. This study fails to show the relation of mentioned institutions INSA and Federal Police with the bank regarding incident information sharing. Recent paper focusing on a given bank information system vulnerability assessment practice done by [9], shows the bank uses IBM Qradar SIEM to collect threat intelligence information, uses phone, E-mail and IBM Control Desk to share or escalate threat information internally. Regarding collaboration with other organizations the paper only explains the practice of the bank in sharing its best practices and showing its SOC for visitors from different organizations. But threat information sharing collaboration with other organizations is not discussed in this paper. The study [68], surveyed the state of cybercrime governance in Ethiopia from three perspectives such cyber security policies and strategies, legislative frameworks, and institutional arrangements. As shown in the result of this survey, most cyber-attack incidents were not reported to the concerning stakeholders. This shows that threat information sharing culture between and across organizations and reporting potential threats to the concerning regulatory bodies in Ethiopia is at its incipient stage. Form these local studies [68][8] we can understand that there is a weak collaboration between stakeholders regarding threat information sharing in Ethiopia, that necessitates research need on cyber incident information sharing collaboration among stakeholders.

The study[69] proposed a threat information sharing framework to improve the cyber security threat information sharing among the collaborating communities. The proposed framework mainly focuses on defining the hierarchical collaboration structure of threat sharing communities by classifying them into five groups. The main gap of this framework is that it fails to adopt automated tools and standards used for threat information sharing as recommended by international guidelines such as NIST Special Publication 800-150 [7], and ITU [62]. The automated platforms and tools for threat information sharing such as malware information sharing platform MISP [58], STIX [43] and TAXII [45] [46] that can enable sharing organizations for better situational awareness and get actionable threat intelligence information. The collaboration group in the proposed framework poses complexity in the threat information sharing process rather than simplifying. For better and timely threat information sharing empowering the super group, implementing collaboration policies, laws and regulations will be effective for the collaborating different sectors. The other limitation in this framework is only focused on the collaboration

structure of the sharing community while ignoring the governance and processes of sharing CTI between stakeholders.

The study [70] proposed a threat sharing collaboration framework for the retail sector by suggesting collaboration layer that is tailored form the NIST Cyber Security Framework (CSF) outlining specific areas for collaborative cyber security by selecting and tailoring subcategories necessary for collaboration. The subcategories from the NIST CSF that were deemed beneficial for collaboration were kept, while the rest were excluded from the framework. This framework fails to incorporate some subcategories related to threat information sharing such as governance of information sharing process, legal and regulatory concerns, access control, trust and security issues. The other gap in this study is that it fails to explicitly present detailed collaborative cybersecurity processes outlining the necessary steps for sharing threat intelligence utilizing those customized subcategories derived from the NIST CSF.

The research [71] tries to propose a conceptual cyber threat information sharing framework focusing on exploring approaches to improve threat information sharing. One of the approaches identified by this study is challenges and incentives for information sharing. The second aspect states about using risk management approaches with mechanisms for sharing and receiving threat information. Thirdly, the paper tried to define the procedural models that define the governance structure, participant roles and responsibilities, and recommendations to establish defined process for threat sharing collaboration. On the fourth stage, it deals with automation and standardization for commonly shared cyber threat information such as vulnerabilities, threat actors, and black/whitelists. This study fails to define and explain the processes of collaboration for CTI sharing, rather than just recommending the need for a clear information collaborative process in general. The paper [50] proposes a cyber threat intelligence sharing platform tailored for defense sector organizations in South Africa. This model identifies four sources of threat data, which are then aggregated into the platform via an API designed to integrate with STIX. The data is classified and interpreted using the TLP, and the resulting threat intelligence is provided for strategic decision making. However, the study's main limitation is its lack of detail on the how the processes are adopted and its failure to align these processes with established models and best practices.

The research based in Indonesia [66] proposes national threat sharing governance framework that can be used as reference that supports the implementation of cybersecurity information sharing for

critical information infrastructure sector in Indonesia. The result of this study consists of three outputs, namely CIS ecosystem, CIS framework that follows process-based approach, and implementation recommendations. The gap of this study, it fails to map with an industry established cyber security frameworks like NIST CSF [54] and intelligence cycle [29] to enhance its applicability, instead of mapping its activity components with Plan-Do-Check-Act (PDCA) cycle, which can be applied for various sectors [72]. The framework proposed by [57] discusses threat information sharing process that primarily focuses on critical infrastructures with the US context. The processes in this framework have a complex nature, implemented in a decentralized approach based on the specific nature of the country.

Title	Author	Finding	Limitations
Cyber Security Practices and Challenges at Selected Infrastructures in Ethiopia: Towards Tailoring Cyber Security Framework	[67]	Tailors' framework to enable CIs respond for cyber threats and proposes common threat storage by CI's and INSA together	• The tailored framework does not show how cyber security units of critical infrastructures collaborate with each other in sharing cyber security threats • It doesn't define the governance of the constructed threat bags
Assessment of Information Security Incident Management Practice in Ethiopian Bank	[8]	Assessment result of information security incident management practices	• Fails to show the relation of mentioned institutions (INSA and Federal Police) with the bank regarding incident information sharing
Towards Improving Information Systems Vulnerability Assessment Practice in an Ethiopian Bank	[9]	Assessment result of information system vulnerability assessment practice	• Threat information sharing collaboration with other organizations is not discussed
A collaborative information sharing framework for community cyber security	[69]	Proposes a threat information sharing framework	• Fails to adopt automated tools and standards used for threat information sharing as recommended by international guidelines • Complexity • Only focused on the collaboration structure ignoring the governance and processes of

			sharing CTI between stakeholders
Collaborative Cyber Security in the Retail Sector A collaborative approach to mitigating cyber security risks in the retail sector	[70]	Proposes a threat sharing collaboration framework for the retail sector	• Fails to incorporate some subcategories related to threat information sharing • Fails to explicitly present detailed collaborative cybersecurity process phases
Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships	[71]	Proposes a conceptual cyber threat information sharing framework	• Fails to define and explain the processes of collaboration for CTI sharing
Developing a Cyber Threat Intelligence sharing platform for South African Organizations	[50]	Proposes a cyber threat intelligence sharing platform tailored for defense sector organizations in South Africa	• Lack of detail on the how the processes are adopted • Fails to align these processes with established models and best practices
The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia	[66]	Proposes national threat sharing governance framework for CII in Indonesia.	• Fails to map with an industry established cyber security frameworks like NIST CSF
Critical Infrastructure Threat Information Sharing Framework A Reference Guide for the Critical Infrastructure Community	[57]	Proposes threat information sharing process for CIs in the US context	• Developed in the US context • Complexity

Table 4: Summary of Related Works

To the best of our knowledge, no prior research has been conducted on cyber threat information sharing specifically framework for collaborative cyber threat information sharing framework for sector specific institutions or at national level in Ethiopia. In addition to fulfilling the gaps identified in the literatures reviewed above, this study could be foundational framework for threat information sharing that encompasses the national collaboration structure, the collaboration

governance and collaboration threat sharing process, and prospective foundational work for future research around threat information sharing in Ethiopia and developing countries.

In general, we have reviewed and presented the most relevant literatures for this study and identified limitations within the related works regarding threat information sharing. The following are the key summary of research gaps identified in the literatures:

- Some proposed frameworks fail to show the collaboration between organizations for sharing cyber threat information.
- Some frameworks are complex to easily implement.
- Some frameworks fail to include threat information sharing process and governance.
- A framework developed based on NIST CSF failed to incorporate some subcategories related to threat sharing and does not explicitly present the desired collaboration process phases.
- Some frameworks fail to show their alignment with an industry established cyber security frameworks, and guidelines.
- Some frameworks are specifically developed for specific context of a country and complex.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1. Overview

This chapter presents the research design and methodology that is utilized to address the research questions formulated in this research. It covers the research process, design, method and sources of relevant data. Additionally, it details the participant selection mechanism, data collection and analysis methods.

3.2. Literature Review

The development of the proposed framework will be based on the review of literature, which will provide a basis to understand current trends and identify potential barriers in Cyber Threat Information (CTI) sharing practices. This review will focus on established CTI sharing frameworks, best practices, guidelines and existing literatures done in Ethiopian context and globally. Assessment of previous research on cybersecurity issues in Ethiopia, including threat information sharing laws and regulations, was another concern of this literature review.

3.3. Research Design

To achieve the research objectives, a qualitative approach was employed. Qualitative research is particularly suitable for research that does not produce measurable or quantifiable results. Its main benefit is that it provides an extensive description and analysis of the research topic, enables diverse participant replies and a wider application [73]. This study's exploratory and qualitative design aims to evaluate Ethiopian organizations current practices for sharing cyber threat information. The findings of this approach provide an in-depth understanding of Ethiopia's cyber threat information sharing gaps and practices. The complicated nature of collaborative cyber threat information sharing activities for collective cyber defense in Ethiopia could be explored because of qualitative methodology [74]. This approach enables us to explore the factors that influence cyber threat information sharing among organizations by providing a deeper insight into the challenges and recommendations.

3.4. Data Collection Methods

Given the type of the research question, a qualitative research approach will be adopted to get more comprehensive understanding of CTI sharing practices in Ethiopia. For this study, data will be collected mainly through semi structured interviews and document analysis. Respondents of the interview process were carefully selected from various stakeholder groups such as regulatory bodies, critical infrastructure organizations, private sector organizations and financial sectors. The interviewees are subject matter experts mainly regarding cybersecurity such as high level managements and senior experts from the selected organizations. The document analysis includes the policy documents, standards, frameworks, guidelines and previously done literature's related with the research topic. The interview questions were open ended, allowing respondents to give detailed explanations and information on the topic. The data collection process involved direct interaction between the researchers and the respondents, with the researchers taking brief notes during the interviews and the interviews transcribed precisely for analysis. The interview questions were derived from various sources, including literature, journal articles, and international standards and best practices. The interviews will provide qualitative insights into the experiences, perspectives and challenges regarding CTI sharing practices among the stakeholders.

3.5. Data Source

The method of purposive sampling was used to identify the data source of this research. This method is a key type of non-probability sampling that involves selection of sample members based on their current role, knowledge, relationships, and expertise related to the research subject [75]. The interviewees for this study were selected from members such as high-level leaders in cybersecurity area such as senior incident monitoring and analysis, and senior professionals in security operation center form the selected organizations. Twelve interviewees from five government, financial and private institutions participated in this research and the respondents selection was based on their experience on the cybersecurity industry.

3.6. Validity and Reliability

For research design and the credibility of research findings, it is crucial to construct validity concerns by making sure a study meets its intended goal [76]. The threat to validity because of the interviewee and researcher bias requires mitigation strategies such as triangulation and member

checking. The triangulation process involves the use of multiple methods to collect data, such as interviews, document analysis, and observations. This increases the data quality and allows us to study from different perspectives. Member checking involves returning data to participants for review to enhance data quality and demonstrate respondents value [75].

We took number of critical actions throughout the research process in order to minimize risks to the validity and reliability of this research process, including:

- Participant selection prioritized respondents with relevant knowledge capable to provide relevant data for the research questions, using our judgment and available evidence to minimize sample bias.
- Our hands on experience with the subject and observations in the field were essential, to provide a unique perspective. The collected data obtained through interviews and document analysis was rigorously examined using the triangulation method.
- We considered the sensitive nature of the research topic and ensured interviews were conducted in a comfortable and convenient time for the interviewee.
- We explained the study's intended use, purpose and data collection methods that built trust between the researchers and participants.

3.7. Ethical Consideration

The development of national collaborative cyber threat information sharing framework required certain key ethical considerations. All possible emphasis given to ethical issues, to have the respondents feel free and collect genuine responses. The name of respondents didn't mention in this research to protect the data privacy and confidentiality. We followed the following ethical considerations during conducting this research:

- We have requested approval through official letter to the selected organizations to collect information
- The anonymity of the respondents was guaranteed
- The anonymity of participated institutions was guaranteed
- The scheduling and interview process was conducted based on the consent of the participants

- All the resources used in this research were properly cited

3.8. Data Analysis

The data analysis method applied in this study involves thematic analysis of the interview transcripts used to identify, organize, and offer insight into patterns of themes in the data set. It helps to identify common and significant patterns in spoken or written topics that must be relevant to specific research goals. This method is chosen for this study because it provides a structured way to code and analyze qualitative data that can be connected to conceptual issues in line with the study's objectives [73].

The thematic analysis used is a six-step process [73]. The first step, familiarization, involves deeply engage with the data (reading and rereading transcripts, listen to audio recordings, making notes of any initial annalistic observations) to identify initial observations and move beyond superficial interpretations. The second step is to generate initial codes. It is a systematic process of identifying and labelling key features of the data relevant to the research question. Coding serves as the initial phase in identifying patterns within the data by clustering similar data segments together. The third step in the thematic analysis process is to search for the themes. It is the step that we cluster together codes to create a likely mapping of key patterns in the data. Reviewing the themes is the fourth step that we check whether the candidate themes exhibit a good 'fit' with the coded data and with the entire data set, and each has a clear, distinct 'essence' or central organizing concept. Step five is about to define and name the identified themes. This process includes creating clear definitions for each theme and selecting appropriate names to ensure conceptual clarity. This step also provides a roadmap for the final report. The final step in the thematic analysis process is to write the report. In this stage, we integrate their analytic narrative with the compiled data extracts. While these themes serve as the organizational framework for the analysis, we draw analytic conclusions across these themes [73]. The analysis for this study will be carried out following the six steps of thematic analysis.

3.9. Chapter Summary

This chapter detailed the research design and methodology for the study on developing a collaborative cyber threat information sharing framework for collective cyber defense in Ethiopia. The use of qualitative approach through in depth interviews, the study aims to gain a thorough

understanding of the research problem. The insights that are gathered from these interviews will offer a clear understanding of on the current status of cyber threat information sharing including the challenges, practices and legal landscape of threat information sharing in Ethiopia. The next chapter will go deeper into the findings to present the data collected and the themes identified during the analysis.

CHAPTER FOUR

DATA PRESENTATION ANALYSIS AND DISCUSSION

4.1. Introduction

In this chapter, data from interviews, analysis and discussion of findings on the collected data presented. The discussion section connects the findings to the research questions presented.

4.2. Respondents Information

The respondents to this research were cyber security directors and senior experts level individuals who play major role in tasks related to threat information sharing at the selected organizations. The main participants of this research were from the selected organizations, in total 12 individuals including senior experts and higher cyber security leaders with extensive experience in the cyber security area such as from security operation center, vulnerability assessment, cyber governance and management, incident response and management and network security. This enabled us to obtain a high-level perspective of senior leaders in cyber threat information sharing.

For confidentiality and ethical considerations, we have anonymized the name of organizations and participants involved in the interview throughout the analysis process.

4.3. Interview Analysis

In this section, the analysis of the qualitative data collected through interviews is presented. The interview responses were analyzed using the steps of thematic analysis as discussed in the research methodology section. The interview responses were transcribed and reviewed, and based on the transcripts, grouped similar data segments form codes by identifying the patterns and then selected codes are categorized into themes addressing the research questions. Six themes were identified from the responses to the interview questions. The identified themes were reviewed and defined so that they can align with the specific objectives of the study. These themes include

- Current practices and methods,
- Challenges on cyber threat information sharing,

- Awareness and training programs,
- Legal and regulatory landscape,
- Regulatory role and collaborations,
- Recommendations for enhancing collaboration.

Based on these themes, the participants interview responses are described and analyzed as follows.

4.3.1. Current Practices and Methods

The assessment of current practices and methods employed by stakeholders in collaborative cyber threat information sharing plays a critical role in shaping the effectiveness and efficiency of such collaborations. Under this theme the interview responses on the current state of threat information sharing among stakeholders such as existence of cyber threat information sharing framework, current practices and methods utilized for sharing cyber threat information are analyzed.

A notable gap identified from the interviews made from high level cyber security managements and experts in all the selected organizations implies the absence of a formal framework within the current practices of cyber threat information sharing in Ethiopia. The lack of a standardized regulatory framework or protocol for threat information sharing can lead to inconsistencies in the effectiveness, quality and timeliness of the shared threat intelligence [7]. To establish precise guidelines, specify roles and responsibilities, and ensure secure and efficient sharing of threat information, a formal and standardized regulatory framework is required [7].

Some of participants involved in the interview mentioned that they are presently implementing the Critical Mass Cyber Security Requirement Standard (CMCSRS) [77] as a guideline within their respective organizations to oversee threat information sharing, despite the absence of a national threat information sharing platform or framework.

One of the three participants, with the role “Cyber Risk Manager” said:

> “*… no, but we are using the critical mass cyber security requirement standard as a guideline to share threat information*”

Integrated cyber defense services division head said:

"As of the latest updates, Ethiopia does not have a well defined, formal framework specifically dedicated to the sharing of cyber threat information among stakeholders…"

Most interview responses indicated their utilization of encryption, secure VPNs for sharing threat information among stakeholders at present. All the respondents agreed that currently they are not using established threat sharing standards. This highlights there is potential gap in the current cyber threat information sharing landscape concerning international best practices and standards such as STIX [43], TAXII [45], MISP[53], and other comparable frameworks intended for sharing cyber threat intelligence among stakeholders. The practice of implementing and using such cyber threat intelligence sharing standards and protocols is critical to improve the interoperability, trust, transparency and reliability and of shared information among stakeholders [7].

One of the respondents said:

"…used NIST SP 800-150 and ISO 9001 as a reference),"

Another respondent with the role of "governance risk and compliance" on the current practice of using cyber threat information sharing standards said:

"There is no formal way or standard for sharing cyber threat information among stakeholders. …common communication channels are being used to do so. Our focus is to get the information by any means possible."

According to the interviews, the stakeholders in Ethiopia leverage various methods to facilitate cyber threat intelligence information sharing. The primary and mostly used methods by organizations in Ethiopia for sharing cyber threat intelligence information involves traditional modes of communication such as email and phone calls. These ways of communication are currently widely used because of their ease of access and familiarity, while can sometimes pose security risks due to potential interception of sensitive information. In addition to the security risks, the dependance on email and phone calls for cyber threat information sharing may limit the ability to efficiently exchange real-time threat information.

As per the responses from some of the interviews, meetings, online platforms such as website portals, social media (Facebook and WhatsApp groups) and formal reports are additional methods of threat information exchange among stakeholders in Ethiopia. The interview responses and our observations indicate that social media and website platforms that are currently in practice serve

as tools for disseminating threat alerts, engaging with the community, and raising awareness about emerging cyber threats. However, the current sharing practice does not include the utilization of online platforms that offer a centralized space for stakeholders to access and contribute to collective threat intelligence, encouraging collaboration and knowledge sharing. The use of centralized online platforms offers various opportunities such as secure messaging, document sharing, and collaborative workspaces, enhances timely access and visibility to shared intelligence information [7][64].

The below are some of the interview responses on the current methodology of sharing information among stakeholders:

> *"In Ethiopia, cyber threat information is shared using several methods, including email, phone communication, web portal by INSA, formal reports and documents"*
>
> *"Most of the time, critical cyber threat information is being shared via email and phones for further explanations."*
>
> *"Sharing is mainly through email and phone"*

In general, the current practices and methods in collaborative cyber threat information sharing in Ethiopia reflects that there are some currently applied approaches and tools by stakeholders. The most frequently utilized means of threat information sharing are traditional approaches such as email and phone calls. There are also mechanisms currently in practice such as formal reports, online web portals and social media, and in person meetings with stakeholders to cyber threat information sharing. The implementation of centralized online platforms, threat sharing standards and formal regulatory frameworks is essential for enhancing the cyber defense capabilities and creating resilient cyber threat intelligence sharing ecosystems in Ethiopia[7] [64]. Accompanying the current practices and tools that currently being used for threat information sharing with standardized national collaborative threat information sharing framework can strengthen the collective defense posture of stakeholders against evolving cyber threats.

4.3.2. Challenges on Cyber Threat Information Sharing

For collective cyber defense collaborative cyber threat information sharing is prevalent in modern cybersecurity strategies, which can enable stakeholders to proactively work against potential cyber-attacks by exchanging relevant and timely intelligence [7]. However, according to the

interviews several challenges hinder the effectiveness of threat information sharing activities in Ethiopia. Based on the collected exploratory interviews, we will go through key challenges faced by stakeholders in Ethiopia such as absence of a formal framework, limited awareness, trust issues hindering information sharing, technical limitations, resource constraints, privacy concerns, coordination challenges, and lack of incentives for sharing.

All the top cyber security leaders and experts interviewed from the selected organizations concluded that one of the main challenges for threat information sharing in Ethiopia is the absence of a formal framework. As per the responses, the absence of standards, and processes, stakeholders cannot be able to share threat information efficiently and securely. A formal framework is essential for defining roles, responsibilities, processes, data formats, encryption standards, and protocols for sharing. Moreover, the implementation of structured cyber threat information sharing framework can enhance the interoperability of shared intelligence, facilitate information sharing, and improve the culture of collaboration between stakeholders.

To quote one the responses from the participants:

> *"Some of the challenges include there is no governing framework for threat information sharing, no adequate awareness, lack of technology and infrastructure on organizations and etc."*

The interview also indicated that limited awareness among the stakeholders and the public about the importance and benefits of cyber threat information sharing because of lack a comprehensive understanding on the value of sharing intelligence leading to underutilization of available cyber threat information sharing platforms and resources. Trust issues, privacy concerns, technical infrastructure and resources constraints, coordination challenges, lack of tangible incentives for sharing cyber threat intelligence among stakeholders are the other challenges raised by interviewees.

The challenges mentioned by the participants on cyber threat information sharing in Ethiopia require rigorous efforts from stakeholders to address effectively. Organizations can improve their collaborative cyber threat information sharing practices and enhance their collective defenses against cyber threats by establishing a formal CTI sharing framework, raising awareness, building trust among stakeholders, overcoming technical limitations, allocating resources, addressing

privacy concerns, improving coordination, and implementing incentives for sharing. Overcoming these challenges requires a coordinated approach, commitment to best practices, and a shared commitment to enhance the culture of threat information sharing and collaboration in the fight against cyber threats.

4.3.3. Awareness and Training Programs

Focusing on the responses provided, we will explore the importance of raising awareness and providing training about threat information exchange among stakeholders. The important topics raised by the interviewees under this theme are limited awareness among the public, and there is relatively better awareness in government and critical infrastructure organizations about threat information sharing. The interview response shows that there are some awareness and training initiatives through workshops, online courses, and collaborative training sessions to offer interactive learning experiences on cybersecurity topics, including threat detection, incident response, secure coding practices, and compliance requirements. Also there have been meetings and conferences that serve as valuable platforms for informing stakeholders about emerging cyber threats, sharing intelligence, and fostering collaboration in cybersecurity initiatives.

Interview respondent with the role "Integrated cyber defense services division head" said:

> *"Yes, awareness and training programs have been provided, including workshops and seminars conducted by INSA and other cybersecurity organizations to educate stakeholders on best practices for cyber threat information sharing, online courses and trainings"*

The other respondent with role "cyber governance manager" also witnessed awareness initiatives done by INSA:

> *"Yes: on the yearly October month program that is organized by INSA, and on the awareness program on the legal framework."*

Also "cyber operation manager" said that he has participated in an awareness session on cyber threat information sharing:

> *"We are invited on different awareness programs one of which is awareness on the law on information sharing and other regulations. I also participated in the policy drafting process"*

The interview indicates that there is better awareness regarding cyber security in higher government and critical infrastructure institutions especially in the telecom and financial sectors. These sectors invest in specialized training programs, cybersecurity certifications, and industry-specific workshops to enhance the skills and expertise of their workforce in combating cyber threats effectively. Even though the awareness of cybersecurity awareness on the critical infrastructure institutions was relatively better, the interviews indicated that there must be more awareness programs crafted to stakeholders specially on collaborative cyber threat information sharing. On the other hand, the interviews emphasized that there is a limited awareness about cybersecurity risks and preventive measures among the public poses a significant challenge to overall cybersecurity readiness. Raising awareness among the public through targeted campaigns, educational resources, and awareness programs can empower individuals to recognize potential threats, adopt secure online practices, and safeguard their personal information from cyber threats and more over to report potential cyber-attacks to the concerning stakeholders.

Two of the respondents said:

> *"... As a knowledgeable guess, financial institutions may have a better experience regarding cyber threat information sharing."*
>
> *"No formal awareness training programs. However, we inform our constituents on meetings and communication channels (email, online platforms)"*

In general, awareness and training programs are essential components of a robust cybersecurity strategy, enabling organizations and the public to build a knowledgeable and resilient workforce capable of defending against evolving cyber threats. A culture of cyber threat information sharing among the community can be created through addressing the current limited cybersecurity awareness among the public, private and public organizations through diverse modalities such as awareness and training programs and campaigns.

4.3.4. Legal and Regulatory Landscape

Based on the responses from the interview participants regarding the current legal and regulatory landscape concerning cyber threat information sharing in Ethiopia, there are points to be noticed that Ethiopia has developed and implemented regulations and standards concerning cybersecurity such as Computer Crime Proclamation (No. 958/2016) [78] that addresses offenses related to

cybercrime, Critical Mass Cyber Security Requirement Standard (CMCSRS) [77], and National Cyber Security Policy of Ethiopia [79]. While existing proclamations and draft laws indicated some progress in addressing cybersecurity concerns, the lack of a detailed regulatory framework specifically that focuses on cyber threat information sharing remains a notable gap. Collaboration with relevant stakeholders and partners, continued development of regulatory frameworks, and alignment with best practices can enhance Ethiopia's cybersecurity posture and facilitate effective information sharing to combat cyber threats. To quote some of the interview responses:

> *"I believe well established regulatory landscape have an impact on the cyber threat sharing behavior among entities. I am not sure if that landscape is implemented currently in Ethiopia."*

> *"Ethiopia's legal and regulatory framework regarding cyber threat information sharing is still evolving, ……. but does not specifically focus on information sharing."*

> *"No regulatory framework particularly mentioned a notion of sharing cyber threat information. But cybercrime proclamation have a dedicated provision to be enforced."*

> *"Ethiopia does not have a specific, comprehensive legal and regulatory framework exclusively dedicated to cyber threat information sharing."*

4.3.5. Regulatory Role and Collaborations

The participants of the interview collectively of highlight that cyber security regulatory body of Ethiopia (INSA's) as a national regulatory plays pivotal role to shape and improve cyber threat information sharing in Ethiopia. Establishment of formal and structured frameworks ensure standardized processes for sharing information securely, training programs and resources that can enhance stakeholder capabilities in understanding cyber threats and active participation in information sharing initiatives, collaboration with sector specific Security Operations Centers (SOCs) to tailor information sharing efforts to industry specific needs, centralized coordination to streamline information sharing, and efficient response to cyber threats across various sectors INSA can enhance the cybersecurity posture of the country and ensure a proactive response to emerging threats.

Initiatives to raise awareness, to build secure communication channels to share cyber threat information, and improve public private partnerships are important for an integrated approach to create a strong culture of sharing cyber threat information in Ethiopia. As Ethiopia's national cyber

security regulatory, INSA can play an critical role to improve the country's capacity to share information about cyber threats by actively engaging in these areas. This will ultimately strengthen the Ethiopia's cybersecurity resilience and proactive response mechanisms.

4.3.6. Recommendations for Enhancing Collaboration

The recommendations provided by the respondents of the interview underscore the multi sided approach is required to enhance collaboration and coordination among stakeholders for effective cyber threat information sharing. Focus to develop structured regulatory framework that provides structure and guidelines for secure cyber threat information sharing that improves partnerships, and improves infrastructure with better tools and platforms for secure information sharing is highlighted as a critical measure to enhance collaboration among stakeholders.

Stakeholders can strengthen their collective cybersecurity efforts and respond more effectively to evolve cyber threats by standard practices, sector specific and cross sector collaboration, and engage in international cooperation and enhance incident response coordination.

Participants stressed the need for increasing training programs and awareness campaigns to educate stakeholders and the public about the significance of threat information sharing. They also indicated the importance to build trust through measures that enhance security, and confidentiality is key to enhance collaboration.

4.4. Finding and Discussion

This study focuses on assessing the current status of cyber threat information sharing in Ethiopia, and examining established international frameworks, standards and practices for sharing threat information with the aim to propose a national collaborative framework for threat information sharing by evaluating and comparing identified gaps and constraints.

4.4.1. What are the current practices, processes, and challenges of collaborative cyber threat intelligence sharing among stakeholders in Ethiopia?

The result of the study collectively indicates that Ethiopia currently does not have a well-established and comprehensive framework dedicated for regulating the sharing of cyber threat information among stakeholders. The Computer Crime Proclamation (No. 958/2016) governs

cybercrime and has brought rules regarding evidence and procedures that can aid in legal proceedings and investigations [78]. The Ethiopian government established a National Cyber Security Policy in 2024 to protect the country's digital infrastructure and to have a secure cyberspace with seven focus areas that includes Legal and Regulatory Framework, Awareness, Capacity Building, research and development, Digital Identity and Personal Data Protection, Key Information Infrastructure Protection, and International and National Cooperation. It provides objectives and tactics for each area and sets up an implementation framework for execution involving various stakeholders [79]. While there are indications that the cyber security legal landscape is evolving with existing strategies, standards, and legal instruments such as Computer Crime Proclamation (No. 958/2016), National Cyber Security Policy, and CMCSRS which is being used as guidelines, a formal governing framework specifically address cyber threat intelligence information sharing among stakeholders lacks at the national level.

The findings show a mix of traditional and digital communication methods currently being employed for sharing cyber threat information among stakeholders in Ethiopia. Email and phone communication appear to be the primary channels for disseminating threat intelligence reports, alerts, updates, and urgent information. There were also collaborative efforts to address cyber threats such as social media, web portals, formal reports, and in-person meetings utilized to facilitate information sharing.

The findings on the current mechanisms for sharing threat information clearly indicate that there is a heavy reliance on traditional methods like email and phone calls. Security, trust, timeliness, scalability, and standards concerns could arise from such dependency. In a collaborative environment, the use of email and phone communication may result in security risks during sharing sensitive threat intelligence information. As the volume and complexity of cyber threat to be shared increases, traditional ways may not be scaled up to accommodate. The result of the study also shows that there is lack of standardized formats and protocols for sharing cyber threat information, which can lead to inconsistencies and difficulties to interpret and utilize shared information.

The current practices on CTI sharing strongly require improvements because of the limited adoption of dedicated online platforms to share cyber threat information and the absence of a comprehensive national framework for cyber threat information sharing. To significantly enhance the effectiveness of collaborative cyber threat information sharing in Ethiopia it requires to

implement secure and standardized methods, leverage dedicated platforms, and establish a national collaboration framework. From the findings on the practice of using standards and protocols for sharing threat intelligence information we understand that the need of developing national framework that aligns with relevant international best practice recommendations from such as ENISA [64], and NIST SP 800-150 [7] and incorporates widely accepted threat sharing standards and platforms such as STIX [43], TAXII [45] and MISP [53] promote interoperability and ensure alignment with global best practices.

Awareness and training programs related to cyber security are being implemented in Ethiopia, but the findings also indicated the need for more structured and comprehensive awareness and training program approaches. While cyber security awareness initiatives indicated by the interview respondents such as National Cybersecurity Month and cyber security stakeholders workshops provide a platform for raising awareness, from the responses we highlight the need for establishing a clear framework that incorporates awareness and training programs to ensure consistency and effectiveness, tailored training programs for different sectors, implementing continuous awareness and training programs, beyond annual campaigns, and regular evaluation on the effectiveness of awareness and training programs.

According to the findings of this research, data privacy and security issues, limited international collaboration, lack of defined proper collaboration channels and centralized platforms, lack of awareness and understanding, lack of trust, resource constraints, regulatory challenges, technical challenges, cultural and organizational barriers, and the lack of a standardized approach for sharing cyber threat information are among the current main challenges in Ethiopia. The reasons why there is lack of trust to provide information regarding cyber threats include concerns about data privacy, lack of governance framework, fear of misuse, and fear of reputational harm. Establishment of comprehensive threat sharing governance framework, enhance awareness and training programs, and improved technological infrastructure capabilities through aggregated efforts from all stakeholders is important to address such concerns. Ethiopia can create a more collaborative landscape for cyber threat intelligence sharing by building trust, provide incentives, and establish clear channels for communication.

4.4.2. What is the role of regulatory bodies in establishing coordinated cyber threat intelligence sharing involving multiple institutions or stakeholders?

To ensure secure cyber space in Ethiopia, the government has established Information Network Security Administration, INSA and Ethiopian Computer Emergency Readiness and Response Team, Ethio-CER2T to protect and respond to cyber attacks target the country and its critical information infrastructures. The Ethio-CER2T unit at INSA will be used as a bridge among all public and private institutions for cybersecurity incidents response [79].

The result of the study emphasizes the important role of regulatory bodies, in particular Information Network Security Administration, INSA, to maintain collaborative cyber threat information sharing framework, enhance collaboration among stakeholders, provide technical resources, promote training and awareness to facilitate an effective cyber threat intelligence information exchange among stakeholders. Moreover, the result of the study pointed that structured approach that includes legal structures and frameworks, adopt international threat information sharing standards and protocols, build trust, enable secure communication channels for collaboration, create a centralized platform, and public private partnerships are essential to build a resilient cyber threat intelligence ecosystem in Ethiopia.

4.4.3. What measures and recommendations should be applied to improve stakeholder collaboration between organizations to effectively share cyber threat intelligence information?

The findings of the study revealed that there are several strategies that can be adopted to improve the current threat information exchange practices to strengthen cybersecurity resilience of the country. The recommendations offered by the interview participants created a roadmap for enhancing collaboration and coordination among stakeholders for effective cyber threat intelligence information sharing. The first critical recommendation collectively offered by respondents is the development of a governing framework for threat information sharing. The findings clearly indicated that there is a need to develop a structured and standardized framework that facilitates the effective collaboration on sharing of threat information between organizations in Ethiopia. Development and implementation of framework for threat sharing will enhance the country's cyber security posture, promote effective threat intelligence exchange, and strengthen collective defense against cyber threats.

Complementing these findings, the 2024 national cyber security policy of Ethiopia mandates the establishment of comprehensive framework at a national level for coordinated threat sharing among stakeholders in alignment with global standards and regulations embraced by the nation. Additionally, it stresses the need to implement comprehensive legal structures govern data collection, analysis, sharing, utilization, storage, and disposal to increase public trust in the country's cyber security capacities [79]. Besides the policy there was a Critical Mass Cyber Security Requirement Standard (CMSCRS) enacted by INSA enforces organizations to create collaborated and coordinated efforts on cyber security information and intelligence at national and sectorial levels [77]. In addition to the national policy and standard, recommendations from international standards organizations have created guidelines and suggestions for collaborative sharing of threat information. Notably, entities like the NIST Special Publication 800-150 (Guide to Cyber Threat Information Sharing)[7] , ITU guide on developing a national cyber security strategy guide 2021[62], and ENISA National Cyber Security Strategies Good Practice Guide[64] have put forward mechanisms for sharing information, often involving central coordinating bodies such as national or industry specific cybersecurity centers. Moreover, recommendations by existing literatures on cyber threat sharing best practices to implement harmonized framework, standards across sectors and nationally for interoperability [49][59][60][37], and literatures on threat sharing frameworks lacking to fill the gap of threat sharing ecosystem in Ethiopia collectively serve as key factors necessitating the proposition of a national cyber threat information sharing framework for collective and collaborative cyber defense.

Experiences from other countries, as shown in the literature review section, to address cyber threat information sharing also shows the necessity to develop national threat information sharing framework using their own approaches to improve the effectiveness and efficiency of cyber threat information sharing [66].

To summarize the factors to propose national cyber threat information sharing framework:

- Ethiopian National Cyber Security Policy [79]
- Critical Mass Cyber Security Requirement Standard [77]
- Recommendations by previous literatures [49][59][60][37]
- Recommendations by international threat information sharing guidelines and best practices [7] [62] [64]

- Gaps identified on reviewed literatures
- Experiences from other countries

These factors offer a strong rationale for the proposal of national cyber threat information sharing framework that is specifically designed to specific context of Ethiopia. The proposed framework will enable coordinated threat information sharing, strengthen legal foundations on cyber threat information sharing, develop cyber defense technical capabilities, raise awareness and capacity building, promote threat sharing partnerships, facilitate international collaboration and also will serve as a strategic guideline to assist national cyber defense efforts. The designed framework is based on international best practices to address the challenges identified as research findings, provide policy directions and recommendations, and will strengthen Ethiopia's cyber resilience and response capabilities in the face of dynamically evolving cyber threats.

The national collaborative cyber threat information sharing framework will enable stakeholders to adopt international threat exchange standards and protocols, enhance partnerships, build trust, enhance technical capabilities, promote awareness, and embrace international cooperation to improve collective cyber security resilience and respond effectively to dynamic and evolving cyber threats. The proposed framework is essential to establish a robust and centralized threat sharing ecosystem that can effectively address the challenges posed by cyber threats in today's interconnected digital world.

4.5. Summary of Findings

NO.	Thematic Areas	Codes
1.	Current Practices and Methods	• Lack of a formal framework for sharing threat information • Use of email, phone calls, online platforms, and formal reports • Lack of specific sharing standards • Methods include meetings, online platforms, and social media
2.	Awareness and Training Program	• Limited awareness among the public • Awareness and training through meetings, workshops, online courses, and collaborative sessions • Higher awareness in government and critical sectors than the public
3.	Legal and Regulatory Landscape	• Evolving legal landscape (CMCSRS, National CS policy, Cybercrime Proclamation etc.)

		• Lack of detailed regulatory framework for threat information sharing
4.	Challenges Faced	• Absence of a formal framework • Limited awareness • Trust issues hindering information sharing • Technical limitations and Resource constraints • Privacy concerns • Coordination challenges • Lack of incentives for sharing
5.	INSA's Role and Collaborations	• Establish frameworks and platforms • Provide training and promoting participation. • Collaboration with sector-specific SOCs and organizations • Centralized coordination • Incident response coordination • Share threat information among sectors • Collaboration across government agencies, private sector, and stakeholders
6.	Recommendations to Enhance Collaboration	• Develop a comprehensive framework • Increase awareness and building trust • Improve infrastructure and technical capabilities • Promote partnerships • Establish legal frameworks • Standardized practices • Facilitate sector specific, cross sector and national collaboration • Advance international collaboration and incident response coordination

Table 5 Summary of findings, includes thematic areas and codes.

4.6. Chapter Summary

In this chapter, the data collected from participants and documents is analyzed and discussed. It covers the respondents' information, challenges encountered during data collection, presentation and analysis of the collected data through interviews and document analysis, and the gaps and challenges in assessing the vulnerability of information systems at the bank.

CHAPTER FIVE

COLLABORATIVE NATIONAL CYBER THREAT INFORMATION SHARING FRAMEWORK

5.1. Introduction

The proposed national cyber threat information sharing framework is an organized approach consisting of governance standards, processes, and structures that enables a secure and efficient exchange of cyber threat intelligence (CTI) between stakeholders across Ethiopia. This framework improves the national cybersecurity posture of the country to enable stakeholders and regulatory bodies to identify, understand, respond and share cyber threats more effectively and collectively. This framework increases a collaborative approach for collective cyber defense by establishing guidelines for trusted information exchange between stakeholders both the public and private sector entities. The framework enables stakeholders to share timely and actionable threat intelligence to mitigate active cyber incidents and improve the overall security posture of the country. The framework is designed to ensure that threat information sharing occurs in a responsible manner, respect data privacy and confidentiality concerns and other legal and trust issues among the sharing community.

5.2. Framework Considerations

In addition to the assessed current CTI sharing status in the country and the research gaps identified in the related works sections, this research considers recommendations from previously done studies and international best practices and guidelines to national CTI sharing framework for seamless cyber threat information sharing among stakeholders. The development of an effective national CTI sharing framework requires the consideration of specific needs and context of the country such as the current cyber security infrastructure, trust status, legal and regulatory landscape, and stakeholders' engagement.

The development of the CTI sharing modalities between the sharing community highly depend on the existing cybersecurity infrastructure of the nation that includes infrastructure capabilities, available resources, and technical systems already in place. Countries with less developed infrastructure may have different requirements than those with developed cybersecurity infrastructure. The proposed framework considers the alignment with the existing technological capabilities.

Clear understanding of the legal landscape within a country is the other critical factor considered for the development of cyber threat information sharing framework that aligns with relevant laws, regulations and policies. The proposed collaborative CTI sharing framework also considers international data protection and privacy laws and regulations specially adheres to the principles in the Critical Mass Cyber Security Requirement Standard (CMCSRS) by Information Network Security Administration, INSA.

Trust between the threat information sharing community such as the public and private sectors is among the fundamental consideration factors to successful threat information sharing framework development. Trust enhances the willingness of organizations to share valuable threat intelligence information with concerning stakeholders. The proposed framework tries to address mechanisms to create trust such as forming guidelines for data privacy and security, and liability.

Engaging all relevant stakeholders, including government institutions, private organizations, and the public, is also an important factor in threat information sharing framework development. The proposed framework involves these stakeholders' collect information as an input and address their respective concerns. This ensures a comprehensive and inclusive approach for the CTI sharing framework development.

The development of a national cyber threat information sharing framework is a strategic endeavor, consideration of these factors enables the proposed framework to address the specific needs and context of the country by creating effective collaboration among stakeholders, to enhance cybersecurity capabilities, and to strengthen the overall national cyber defense resilience.

5.3. Mapping NIST SCF

The proposed national cyber threat information sharing framework is developed based on the NIST Cybersecurity Framework (NIST CSF) [54]. The proposed framework components are mapped to selected NIST CSF subcategories related to threat information sharing process and governance. The NIST CSF has crucial characteristics [70] such as completeness, interoperability with other frameworks, adaptability regarding organization size and completeness in that each of the controls in the NIST CSF are mapped with references to other industry-recognized standards, including COBIT 5, NIST SP 800-53, and ISO/IEC 27001:2013, are provided. The proposed national threat information sharing framework adopted NIST CSF subcategories especially related with the governance of threat intelligence collaboration.

One of the contributions of this study is mapping subcategories from the NIST CSF that are suitable for the development of national CTI sharing framework. Subcategories related to threat information sharing processes, threat information sharing governance, training and awareness, and feedback and continuous improvement of threat sharing are embedded to each of the components of the proposed framework. Detail description of mapped categories and subcategories from the NIST CSF can be found at Appendix C.

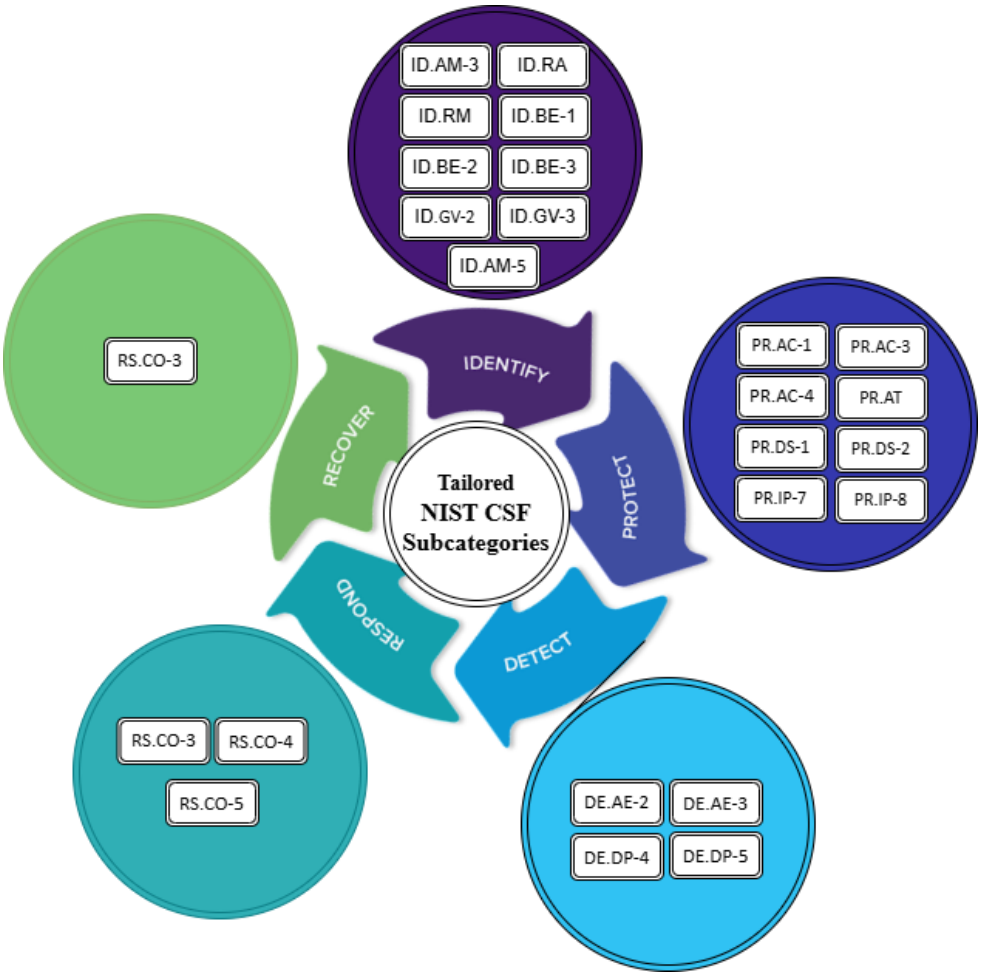

Figure 7: The Mapped Subcategories form the NIST SCF

5.4. The Framework Components

The main contribution of this research is the development of the CTI sharing framework with three critical components, namely the collaboration structure, the collaboration process and the collaboration governance. These three components of the proposed framework are mainly based on the NIST CSF, the intelligence lifecycle and the current cyber governance structure of the country.

The first layer of the proposed framework is the collaboration structure which outlines hierarchical communication between different levels of stakeholders. This layer establishes the administrative structure and identifies the key points of contact, such as national CTI sharing hub, sector-specific SOCs with their hub units, at various levels of government institutions, private sectors, and the public. The purpose of the collaboration structure is to facilitate effective communication and coordination to ensure that information flows efficiently among the sharing community.

The second layer is the collaboration process which addresses the process of sharing the CTI. The CTI sharing process involves the planning, collection, analysis, and dissemination of exchanging CTI among stakeholders. It also covers feedback and continuous improvement of CTI sharing among organizations. By following this process and recommendations in this layer, stakeholders can ensure that relevant and actionable threat intelligence is shared securely and efficiently, which enables them to be proactive to mitigate threats and to make informed decisions. To depict the collaboration process stages of the proposed framework, the intelligence cycle as implemented in the literatures adopted and customized, and subcategories from the NIST CSF were mapped.

The third layer of the proposed framework is the collaboration governance which focuses on the governance issues during sharing of CTI information. It recommends the establishment of policies and regulations that govern the sharing of CTI. This layer clarifies the trust issues and, roles and responsibilities and of stakeholders involved in the sharing process. The alignment of CTI sharing activities with legal and regulatory frameworks is ensured at the governance layer of the framework.

The proposed collaborative CTI sharing framework as shown in *Figure 7*, with its three components, provides a structured approach to facilitate seamless communication by defining administrative structure, to define the CTI sharing processes between stakeholders, and to establish the CTI sharing governance mechanisms.

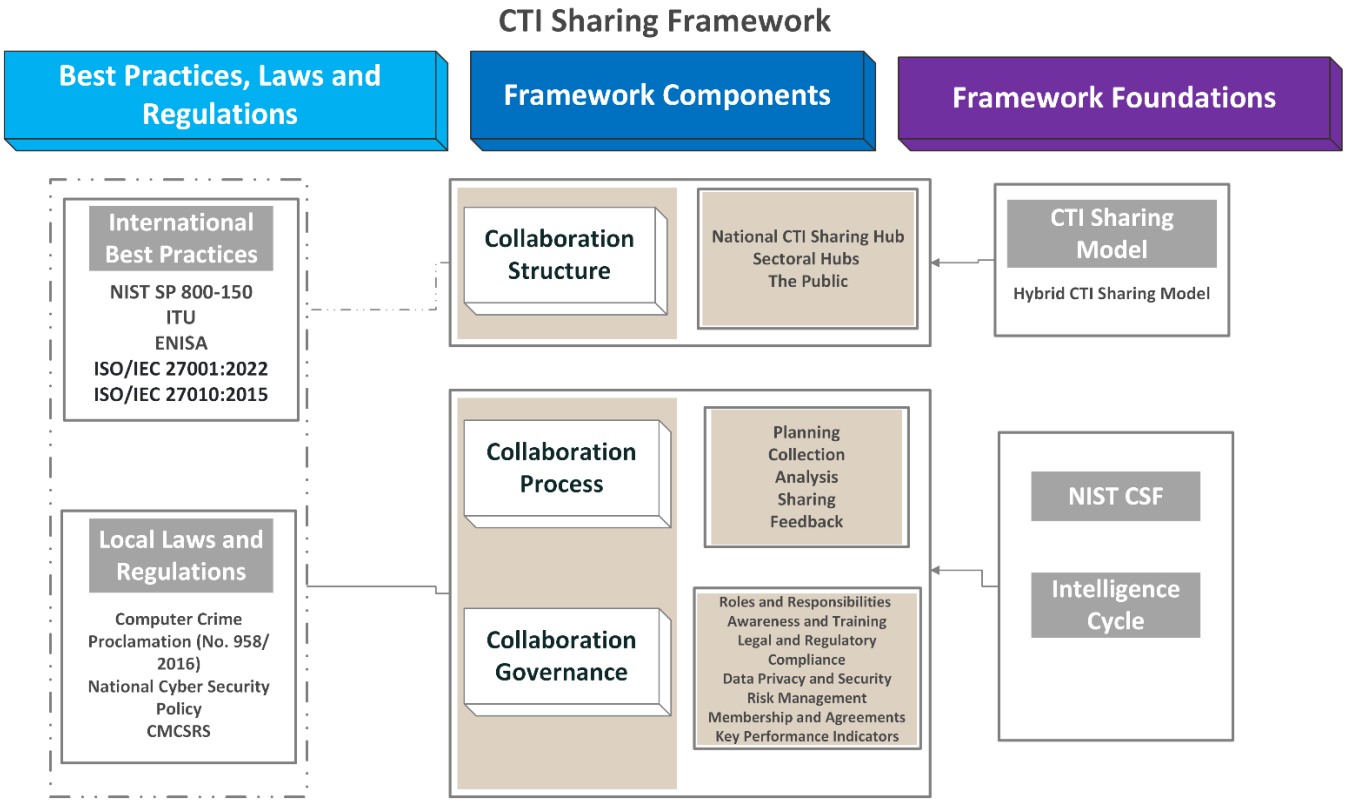

Figure 8: The Collaborative CTI Sharing Framework

5.4.1. The Collaboration Structure

The formation of CTI sharing hubs or structures at different levels is crucial for effective cyber threat information sharing to enhance the current CTI exchange capabilities and to strengthen the collective defense against cyber threats. The hubs function as centralized fusion centers to collect, analyze, and disseminate CTI to relevant stakeholders.

Countries follow their own specific approaches [66], as indicated in literature review section, for threat information sharing according to the specific context of each country. The US uses decentralized approach [57] which resembles to point to point (peer to peer) sharing model, using formal and informal channels to share threat information, whereas the UK emphasizes the role of

the National Cyber Security Centre (NCSC) [65] as a central coordinating body for cybersecurity efforts by following more centralized approach in which the government takes the leading role. Successful national threat sharing frameworks often have unique features and approaches developed to their specific contexts such as political, economic, technological, and cultural context of each country to ensure the framework relevant, effective, actionable, and sustainable.

The collaboration structure component of the proposed national CTI sharing framework consists of the National CTI Sharing Hub, Sectoral CTI Sharing Hubs, and Regional CTI Sharing Hubs that facilitate the sharing of Cyber Threat Intelligence (CTI). This administrative collaboration structure follows the current federal structure of the Ethiopia for the ease of communication between the federal government cyber security governing organization (INSA) with the regional governments and other sectors across the country.

The CTI sharing collaboration structure of the proposed framework accommodates ***hybrid CTI sharing model*** [80] that includes both the hub and spoke model and peer to peer model as needed. The structure accommodates both the hub and spoke and peer to peer models providing flexibility in CTI sharing by allowing organizations to benefit from the centralized resources and analysis provided by the central hubs and enables direct collaboration between peers.

The hub and spoke model [80] involve centralized CTI sharing hubs (national or sectoral hubs) which acting as central collaboration units for collecting, analyzing, and disseminating CTI. These hubs are the primary repositories of CTI that facilitate the exchange of information between different entities. They aggregate CTI from various sources including peer organizations and distribute relevant information to organizations or sectoral hubs. Organizations will entertain direct CTI sharing between each other based on their specific needs and relationships in the peer to peer model [80]. This can be done through establishing bilateral or multilateral agreements to share threat intelligence, indicators of compromise, and other relevant information to defend their critical infrastructure assets from emerging cyber attacks.

The effectiveness of CTI sharing among the CTI sharing ecosystem requires trust, formal and acceptable processes and procedures, and adherence to privacy, security, and legal requirements. The collaborative CTI sharing ecosystem that enhances cybersecurity posture, enables proactive cyber defense, and improves timely and actionable threat intelligence for timely response to

cybersecurity incidents is result of collaborative effort of CTI sharing hubs along with individual organizations and the public.

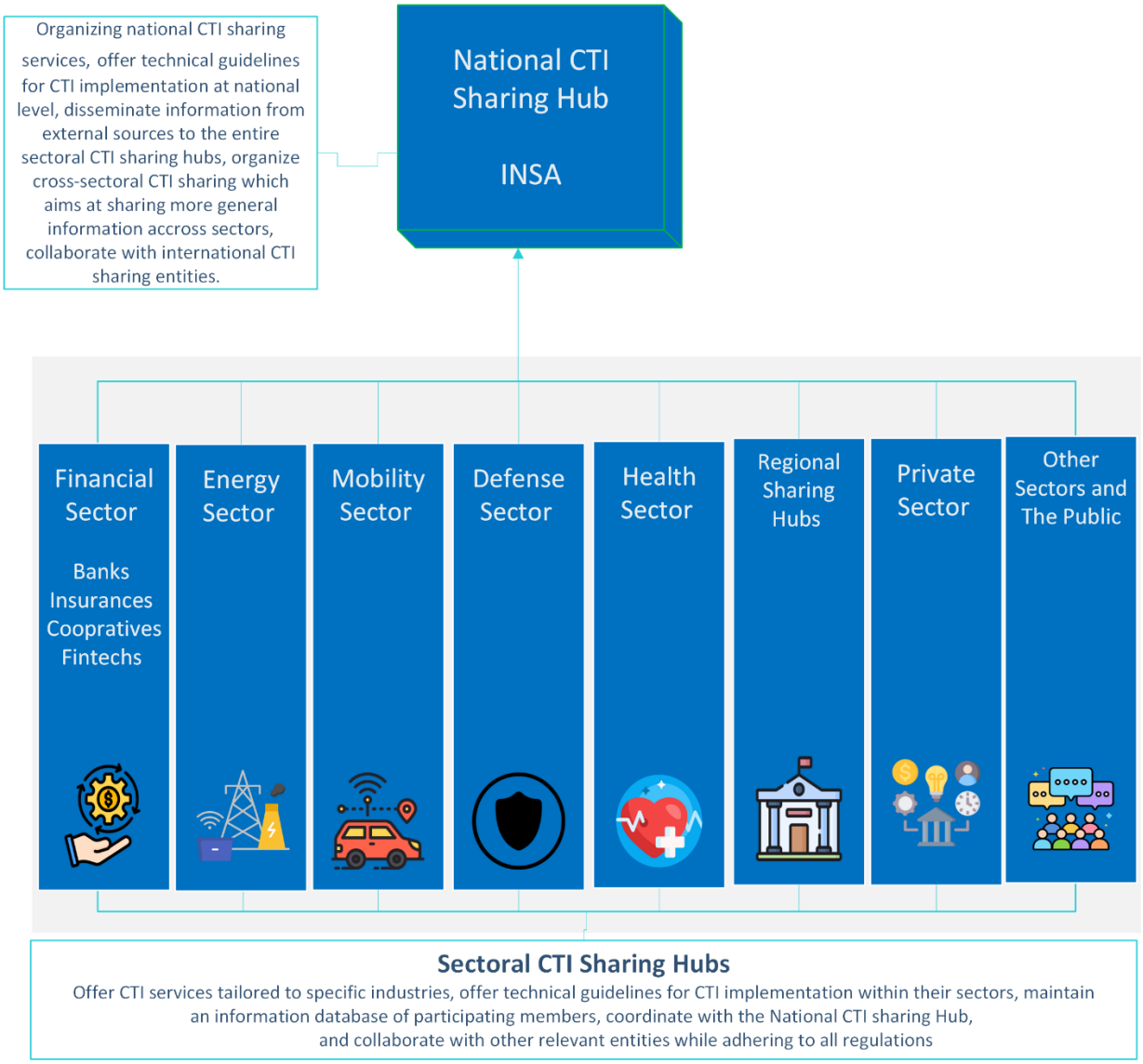

Figure 9: The Collaboration Structure

5.4.2. The Collaboration Process

As discussed widely in the related works and literature review section regarding previously proposed frameworks on threat information sharing like [57] and intelligence cycle implemented in literatures [29][30][32][31] are used as a benchmark for proposing the collaboration process

layer and the gaps identified on the reviewed literatures were the factors that initiated us to propose a framework for threat information sharing in Ethiopia.

The process of sharing the cyber threat information is addressed at the collaboration process layer of the proposed framework. It plays a key role to ensure relevant and actionable threat intelligence is effectively and securely exchanged among stakeholders. The collaboration process of the proposed framework covers steps such as collection, analysis, and dissemination of threat information. The mechanisms of threat information sharing such as protocols, tools and methods used, standards, and formats of exchanging CTI among stakeholders are defined in this layer. This layer also covers feedback and continuous improvement of CTI sharing among organizations.

As depicted on *figure 9*, the specific NIST CSF subcategories that are specifically mapped to the collaboration process layer of the proposed cyber threat intelligence information sharing framework. In the context of the proposed cyber threat intelligence information sharing framework, the collaboration process layer focuses on the following processes that can be mapped to subcategories derived from the NIST CSF. The steps within the collaboration process will enable stakeholders to collect, analyze, and disseminate CTI in an effective manner and securely. This will improve the current overall cybersecurity defense capabilities to ensure proactive threat detection and informed decision-making. By incorporating the selected NIST CSF subcategories into the collaboration process layer of the proposed framework, it ensures a structured and systematic approach to cyber threat intelligence information sharing among stakeholders, enables organizations to effectively identify, analyze, share, and respond to cyber threats.

The collaboration process component of the proposed framework in this study adopts five phases of the intelligence cycle namely planning, collection, analysis, sharing and feedback. By mapping each step of the collaboration process to specific NIST CSF subcategories, the framework proposed in this study ensures that threat information sharing among stakeholders is structured, comprehensive, and aligned with recognized cybersecurity standards. This approach will strongly help organizations systematically manage and share threat intelligence information to enhance their overall cybersecurity posture. The detail description of the mapped NIST CSF subcategories for the collaboration process layer presented at Appendix D.

	CTI Framework (Literatures)

CTI Sharing Process	[29]	[30]	[32]	[31]
Planning	✓	✓	✓	✓
Collection	✓	✓	✓	✓
Processing	✓	✓	✕	✓
Analysis	✓	✓	✓	✓
Sharing	✓	✓	✓	✓
Feedback	✕	✓	✕	✓

Table 6: Comparing literatures adopted the intelligence cycle

Planning

Planning is the first phase of the CTI sharing process that involves identifying main stakeholders and defining the organization's objectives, priorities, and requirements regarding threat intelligence. A proper plan on how to collect threat information based on the organizations need from different sources abiding with laws and regulations enacted by concerned authorities. This step is important phase of the collaboration process because its output will be foundation for the following stages [32] [54].

Collection

This process relates to the methods and techniques used to gather cyber threat intelligence from various sources, such as internal logs, external threat feeds, and open-source information. It involves obtaining details on threats, vulnerabilities, and incidents from involved stakeholders and other relevant sources of threat information. This process should consider capabilities of automation to access timely and up-to-date information from sources.

Analysis

It is the process of analyzing and interpreting the collected threat intelligence to identify patterns, trends, indicators of compromise (IOCs) and potential threats. The threats identified based on their severity and impact level are prioritized and the collected CTI is analyzed to extract meaningful insights and identify potential threats and vulnerabilities. This process aligns with the NIST Cybersecurity Framework (CSF) subcategories DE.AE-2 (Threat and Vulnerability Data are Aggregated) and DE.AE-3 (Event Data are Aggregated and Correlated from Multiple Sources) under the Detection (DE) function.

The analysis process also aligns with the ID.AM-5 of NIST CSF. This involves the classification of CTI to define a standardized taxonomy, to organize and to categorize for promoting an effective search, retrieval, and correlation of threat information across the sharing community. This enables stakeholders to quickly identify relevant threat information based on attributes such as threat type, target, attack vectors or location. Using threat sharing standard taxonomies, such as STIX or CAPEC (Common Attack Pattern Enumeration and Classification) [44], can promote integration and ease of threat information exchange.

Sharing

Sharing cyber threat information is the third process of collaborative process layer of the proposed framework. This process encompasses the methods and protocols used to securely share threat intelligence with authorized stakeholders, both within and outside the organization. Mechanisms and channels for CTI dissemination to relevant stakeholders are determined. This includes secure channels for communication, platforms for sharing and mechanisms for sharing. The collected cyber threat information from various sources is identified and analyzed to identify patterns, trends, and potential threats. It involves the dissemination of analyzed threat data about potential threats to relevant stakeholders such as peer organizations, sectorial hubs or national threat information sharing hubs. The threat information sharing can be done in various channels such as threat intelligence sharing platforms, or direct communication between peer organizations, sectorial SOC's or national cyber threat sharing hub. Indicators of Compromise (IoCs), Tactics, Techniques, and Procedures (TTPs), Threat Intelligence Reports, Best Practices and Mitigation Strategies were among some of threat intelligence information's to be shared between stakeholders.

Cyber threat information can be shared both manually and automatically. Manual sharing includes techniques such as mailing lists, newsgroups, web portals, and online forums, usually requires human involvement. Manual threat information sharing has some advantages such as to build relationship with the community, to provide context and thorough explanations, and facilitate conversations that may understanding of cyber threats. These traditional approaches require active involvement from human, that causes increased expense for human resources and limit the volume and scope of information that can be addressed efficiently [81].

On the other hand, automatic cyber threat information sharing will use automated tools for enhancing the sharing process. This also includes things like TAXII (Trusted Automated eXchange of Indicator Information) [44] that defines how threat information is transported, STIX (Structured Threat Information eXpression) [44] specifies what the threat information includes, MISP (Malware Information Sharing Platform) an open source platform that supports to share, store, correlate and analyze threat information [53] and other tools that enable organizations and sharing hubs to collect, analyze, and distribute threat information in an automated manner. The use of automated tools in threat information sharing helps to reduce resource costs, to handle large volume of data, reduce potential human error, and also it makes it possible to respond to threats more quickly [7].

The NIST CSF subcategories DE.DP-4, RS.CO-3, RS.CO-4, RS.CO-5, and RC.CO-3 are particularly mapped to align with share information process of the collaboration process layer. These subcategories mainly focus on the importance of communication and collaboration among stakeholders on cyber threat information sharing. They serve as a framework for all parties involved organizations to be aware and act together to successfully handle cyber threats.

Feedback and Continuous Improvement

This process of the collaboration process layer highlights the need for continuous monitoring, evaluation, and feedback to refine and improve the threat intelligence sharing processes and mechanisms. This process helps to identify areas for enhancement, address emerging challenges, and incorporate lessons learned. From incidents that have occurred in other organizations, stakeholders can gain insights into emerging risks, attack vectors, and vulnerabilities. This knowledge can be applied to enhance both protection processes (PR.IP-7) and detection processes (DE.DP-5). By actively sharing lessons learned on the protection and detection of cybersecurity threats and collaborating with other stakeholders, organizations can collectively strengthen their cybersecurity defenses and stay ahead of evolving cyber threats.

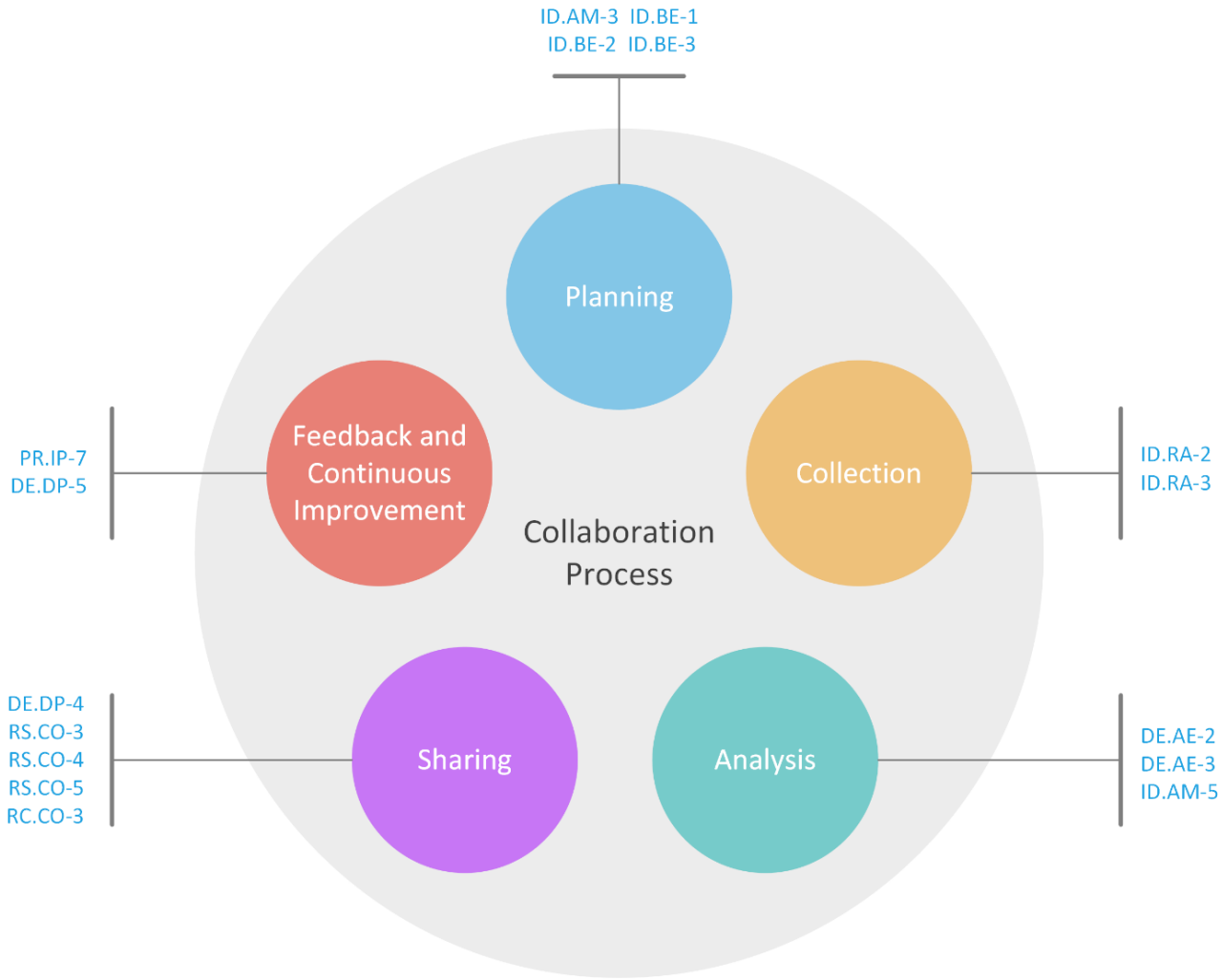

Figure 10: The Collaboration Process

The remaining NIST CSF subcategories selected for the proposed cyber threat intelligence information sharing framework are covered in the succeeding layer which deals with governance of the collaboration on cyber threat information sharing. The collaboration governance layer focuses on establishing rules, procedures, and control mechanisms to ensure the smooth and secure collaboration process for sharing cyber threats between different organizations.

5.4.3. The Collaboration Governance

The collaborative governance layer is one of the important components of the proposed national cyber threat information sharing framework and contribution of this research, focuses on overseeing the exchange of cyber threat data among the members of the sharing community.

Roles and responsibilities of all concerning stakeholders, awareness and training for participants in threat information sharing, legal and regulatory compliance by the participating stakeholders, data privacy and security of the CTI, risk assessment and management, memberships and agreements between stakeholders, KPI's are components of this layer. Each of these components are then mapped to mapped subcategories from the NIST cybersecurity framework [54] which are crucial for establishing effective governance mechanisms between stakeholders involved in threat information sharing, as depicted in figure 10 and appendix D, for instance the roles and responsibilities component is mapped with the ID.BE-1, ID.BE-2 and ID.GV-2.

Figure 11: The Collaboration Governance

Awareness and Training

Awareness and training are an important component of the collaborative governance layer, which should be regularly offered to participating organizations in threat information sharing, and the public. The purpose of awareness and training is to emphasize the importance of sharing cyber

threat information and ensure that organizations are informed about its significance. And also, it ensures that stakeholders are well informed, trained, and equipped to handle and share cyber threat information securely, on legal and policy considerations, contribute to a more effective and collaborative cybersecurity ecosystem. The responsibility to provide awareness training programs lies with organizations, sectorial hubs, and national threat information sharing hubs, each within their respective roles and responsibility on cyber threat information sharing. The associated NIST CSF subcategory that aligns with the awareness and training component of the collaboration governance layer is the PR.AT-1.

Roles and responsibilities

Collaborative governance of cyber threat information sharing involves various stakeholders who have different roles and responsibilities. *Table 7* outlining the roles and responsibilities for effective collaborative governance among stakeholders.

Stakeholder	**Role and Responsibilities**
National CTI Sharing Hub, INSA (Ethio-CERT)	The national CTI sharing Hub is the core for the coordination on cyber threat intelligence at the national level • Develop policies, guidelines, and frameworks for cyber threat information sharing • Provide legal and regulatory guidance on cyber threat information sharing • Promote and coordinate collaborative cyber threat information sharing among stakeholders at national level • Foster to establish clear agreements to ensure effective cyber threat information sharing and collaboration among stakeholders • Provide or recommend appropriate platforms, tools, and mechanisms for secure cyber threat information sharing • Collect, analyze, and disseminate cross-sector threat intelligence. • Support incident response and recovery efforts on organizations, and sectorial hubs • Continually improve the CTI sharing process

	• Develop and provide awareness and training programs to create a conducive sharing environment
Sectorial Hubs (Sectorial SOC's)	• Coordinate collaborative cyber threat information sharing among stakeholders within specific sectors or industries. • Collect, analyze, and disseminate sector-specific threat intelligence. • Coordinate incident response and mitigation efforts within the sector. • Foster collaboration and cooperation among member organizations • Collaborate with the National CTI Sharing Hub to contribute to and benefit from the national hub by information exchange, coordinate responses, leveraging expertise, participating in awareness and trainings, and adopting best practices.
Regional CTI Sharing Hubs	Regional CTI Sharing Hubs that shall operate at each region of the country primarily operate at a regional level to facilitate the collaboration of sharing CTI among regional organizations. They establish connections with the national CTI sharing hub and serve as intermediaries between regional government institutions and the national CTI sharing hub. The main responsibility of regional hubs is to share timely and actionable CTI information with stakeholders and the public in the region.
Private Sector CTI Sharing Hubs	Private Sector CTI Sharing Hubs facilitate the cooperation on threat information sharing among private sector organizations. They serve as centralized platforms of communication with the national hub and other sectors to collectively address threats and vulnerabilities, effective response to incidents, share best practices, and enhance the cybersecurity defense posture of private firms.
Organizations (Public and Private)	• Actively contribute cyber threat information and intelligence for stakeholders. • Share incident details, indicators of compromise, and best practices with stakeholders. • Collaborate with other organizations and stakeholders. • Implement security measures based on shared intelligence. • Report incidents and breaches to appropriate authorities.

Research Institutions	• Establish a training and awareness programs to ensure that participating entities understand their roles and responsibilities in the CTI sharing framework. • Conduct research on cyber threats and trends and share research findings and insights. • Contribute to the development of best practices and guidelines on threat information sharing. • Collaborate with stakeholders to enhance cyber threat information sharing
The Public	The involvement of the public in cyber threat intelligence (CTI) information sharing is critical to create a resilient and proactive cybersecurity ecosystem. Among the crucial roles that the public society plays in the sharing of CTI are report cyber incidents they encounter to the relevant hubs or institutions, share IOCs that include IP addresses, domains, hashes, or other artifacts associated with malicious activities, public awareness, and education initiatives, and support Open-Source Intelligence (OSINT) from sources like social media, forums, news outlets, and public databases. In general, the participation of the public enhances the effectiveness of CTI exchange and strengthens the overall cybersecurity posture of the community.

Table 7: Roles and Responsibilities

Membership and Agreements

There should be a sounding requirement for joining a CTI sharing ecosystem. A given organization should fulfill the membership criteria provided by the national CTI sharing hub and the respective sectoral hubs. Relevance can be one of the criteria to be a member of CTI sharing community. If the organization requests to be a member of a CTI sharing community related to the finance sector, the relevance criteria would be operating in the financial industry. Commitment to collaboration, legal and ethical compliance, and trustworthiness could also be an additional criterion that organizations or individuals may need to be a member of a cyber threat information sharing community. The organizations or individuals could gain understanding about the requirements of the community by reviewing its guidelines, policies, and membership criteria.

Key Performance Indicators (KPIs)

Key performance indicators (KPIs) for collaborative cyber threat information sharing framework are important to evaluate the effectiveness of collaborative cyber threat information sharing among the stakeholders. As shown on *table 8*, 7 key performance indicators are selected according to international guides such as [7] [82].

No.	KPIs	Description
1.	Timeliness	To measure how quickly threat information is disseminated among stakeholders [7] [82].
2.	Relevance	To assess how significant the shared threat information is to the recipient's context [7] [82].
3.	Accuracy of CTI	To evaluate the correctness of the shared threat information [7] [82]
4.	Specific and Actionable	Threat indicators should provide clear descriptions of observable events that threat information sharing community can use to detect threats and minimize false positives/negatives. Threat indicators should also provide enough threat information and context to allow recipients to develop a suitable response [7] [82]
5.	Participation Rate	This measures that many organizations are actively participate and contribute to the threat information sharing community [7].
6.	Impact	to assess the effect of the shared information to reduce risk or improve response [7] [82].
7.	Feedback	To evaluates feedback from participants regarding the quality and usefulness of the shared information [7] [82]

Table 8: Key performance indicators of collaborative CTI sharing

5.5. Validation

This section describes the validation of collaborative cyber threat information sharing framework for Ethiopia. In most academic research [83], expert review is the widely used methodology that involves obtaining professional feedback from domain experts to assess the framework's relevance, feasibility and applicability for the intended research purpose. In this research the expert review helped us to get important feedback to identify areas for improvement.

5.5.1. Participants Selection

We have contacted three cybersecurity experts above 8 years' work experience to evaluate the proposed collaborative cyber threat information sharing framework. The experts include cyber security division head, and senior cyber security experts which have credible industry level certifications that makes them right candidates for the validation of the proposed framework. To abide with the ethical considerations, the names of these respondents is anonymized. The experts received a detailed document that illustrates the structure and components of the proposed national cybersecurity threat information sharing framework.

5.5.2. Evaluation Criteria and Results

The domain experts were asked to evaluate the proposed framework based on the following interview questions.

- Can you describe how easy the framework to understand?
- How relevant and applicable is the proposed framework?
- How complete is the proposed framework?

Based on the above questions, the summary of each of the expert's evaluation is described as follows:

- Can you describe how easy the framework to understand? Respondent I reviewed the proposed framework, while appreciating the overall structure of the framework, gave feedback as "*the framework is easy to understand with clear structure, but I strongly recommend if the components of the framework are clearly defined on the architectural design part".* The other two of the respondents gave similar response by saying that the framework is easily understandable.
- How relevant and applicable is the proposed framework? Respondent I assured the relevance of the framework by saying, "*the framework is highly relevant, since there is no such framework in Ethiopia previously proposed for threat intelligence information sharing*". Respondent II and III agreed on its relevance and emphasized on its applicability by appreciating the framework's compliance with international standards and developed mainly based on the NIST cyber security framework. Respondent III suggested including

guidelines for different types of organizations can tailor the framework to their specific needs.

- How complete is the proposed framework? One of the three respondents critically commented on the completeness of the originally shared framework, saying that the proposed framework does not show the interaction between the framework components. This helped us to redesign the framework, so that the components are clearly defined and interactions among the framework components, the adopted standards, laws and regulations are outlined in an understandable manner. All the three participants selected for this evaluation reviewed the proposed framework to evaluate its completeness. They all mentioned that the framework components (collaboration structure, process and governance) indicate the framework is complete by fulfilling all aspects from technical perspective such as the processes and mechanisms of threat sharing to governance perspective including legal and regulatory compliance. Two of the experts ensured that the framework aligns with national and international cybersecurity regulations, but they also advised a thorough review to ensure compliance and avoid potential legal issues.

The expert's evaluation on the proposed national cybersecurity threat information sharing framework were generally positive and valid to fil the current limitation in threat information sharing among stakeholders. They appreciated the detailed structure and comprehensive components outlined in the document. The respondents also provided constructive feedback on the areas that could be improved, such as enhancing clarity on the components as the framework architecture and ensuring the framework's adaptability to different organizational contexts. However, the proposed framework needs to be tested in real-world scenarios and further researched to allow for ongoing improvements.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1. Conclusion and Recommendations

This research proposes a collaborative national framework for sharing cyber threat information, designed to enhance collective cyber defense efforts and improve the existing culture of information sharing among organizations in Ethiopia. To fulfill this objective, we evaluated current practices, challenges, and recommendations related to cyber threat information exchange through interviews and document reviews from selected organizations. The proposed framework integrated insights from the interview analysis, document reviews from current national cyber security legal frameworks and guidelines and drawn inspiration from international standards, frameworks and best practices. The following conclusions are drawn from the study's analysis and findings:

- Ethiopia currently does not have a well-established and comprehensive framework dedicated for regulating the sharing of cyber threat information among stakeholders.
- Cyber threat information sharing in Ethiopia relies on a combination of traditional (email, phone calls, in-person meetings) and social media, web portals, and formal reports communication methods.
- Awareness and training programs related to cyber security are being implemented in Ethiopia, but the findings also indicated the need for more structured and comprehensive awareness and training program approaches for especially regarding cyber threat information sharing.
- The current main challenges regarding cyber threat information sharing in Ethiopia include the absence of a comprehensive and standardized approach, limited awareness and understanding, trust issues, resource constraints, regulatory challenges, technical challenges, cultural and organizational barriers, data privacy and security concerns, limited

international collaboration, and the lack of defined proper collaboration channels and centralized platforms.

- The result of the study emphasizes the important role of regulatory bodies, particularly Information Network Security Administration, INSA, in establishing collaborative framework, enhancing collaboration among stakeholders, providing technical resources, promoting training and awareness to facilitate an effective cyber threat intelligence information exchange among stakeholders.
- Development and implementation of a framework for threat sharing will enhance the country's cyber security posture, promote effective threat intelligence exchange, and strengthen collective defense against cyber threats.

6.2. Limitation and Future Work

This study lays the groundwork for future research in the CTI sharing area because there is no existing research on cyber threat information sharing among stakeholders in Ethiopia. The research proposes a framework regarding sharing cyber threat information in Ethiopia, suggesting that future studies could validate this framework in practical contexts.

The primary focus of this study lies to develop framework of threat intelligence sharing. The development or customization of cyber threat intelligence standards, ontologies, taxonomies, and schemas for automated CTI sharing falls beyond the scope of this research.

Based on this study future researches can further refine and implement advanced and automated threat intelligence sharing platforms and tools specifically designed for Ethiopian context in accordance with established international best practices and standards that can significantly contribute to the threat information sharing ecosystem. By addressing issues beyond the current scope of this research, such efforts will increase understanding of efficient cyber threat information sharing mechanisms. These advancements would not only improve Ethiopia's collaborative cybersecurity efforts effectiveness but also provide valuable insights into the overall landscape of cybersecurity practices globally.

REFERENCES

[1] D. P. F. Möller, *Cybersecurity in Digital Transformation*. 2020. [Online]. Available: http://link.springer.com/10.1007/978-3-030-60570-4

[2] G. Vial, “Understanding digital transformation: A review and a research agenda,” 2019.

[3] IBM, “Cost of a Data Breach Report 2024,” 2024.

[4] ENISA, *ENISA Threat Landscape 2021*, no. October. 2021.

[5] Interpol, “African cyberthreat assessment report: Interpol’s key Insight into Cybercrime in Africa,” *Interpol*, no. October, pp. 1–34, 2021, [Online]. Available: https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

[6] ENA, “Over 1600 Cyber Attacks Thwarted in First Quarter of Ethiopian Fiscal Year,” 2022.

[7] C. Johnson and D. Waltermire, “NIST Special Publication 800-150 (Draft) Guide to Cyber Threat Information Sharing,” vol. 150, p. 73, 2014, [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[8] T. YOHANNES, “ASSESSMENT OF INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICE IN ETHIOPIAN BANK,” pp. 1–26, 2018.

[9] A. Abay, “Towards Improving Information Systems Vulnerability Assessment Practice in an Ethiopian Bank,” no. June, 2021.

[10] Dr. S. Ozarslan, “Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022,” 2022.

[11] N. Tariq, “Impact of Cyberattacks on Financial Institutions,” *Journal of Internet Banking and Commerce*, vol. 23, no. 2, pp. 1–11, 2018.

[12] A. Ker, “RISING CYBER THREATS TARGETING THE BANK- ING SECTOR,” 2022.

[13] Akamai technologies, “Phishing for finance,” vol. 7, no. 2, 2021.

[14] “IBM: X-Force Threat Intelligence Index,” *Computer Fraud & Security*, vol. 2022, no. 3, 2022, doi: 10.12968/s1361-3723(22)70561-1.

[15] E. Monitor and D. N. from Ethiopia, “INSA Thwarts Over 1,600 Cyber Attack Attempts on Ethiopia,” Addis Ababa, 2022.

[16] L. Gotseva Petkova, “Cybersecurity Trends,” vol. 140, no. 4, pp. 137–140, 2021.

[17] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, “A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions,” *ACM Comput Surv*, vol. 1, no. 1, 2022, doi: 10.1145/3514229.

[18] M. Henriquez, “Banking industry sees 1318% increase in ransomware attacks in 2021”.

[19] D. Y. Kao, S. C. Hsiao, and R. Tso, “Analyzing WannaCry Ransomware Considering the Weapons and Exploits,” *International Conference on Advanced Communication Technology, ICACT*, vol. 2019-Febru, no. 1, pp. 1098–1107, 2019, doi: 10.23919/ICACT.2019.8702049.

[20] L. Hadlington, “Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom,” *International Journal of Cyber Criminology*, vol. 12(1), no. 1, pp. 262–274, 2018, doi: 10.5281/zenodo.495776.

[21] H. Schulze, “Insider Threat: 2020 Report,” *Cybersecurity Insiders*, pp. 1–24, 2020.

[22] M. Guarascio, N. Cassavia, F. S. Pisani, and G. Manco, “Boosting Cyber-Threat Intelligence via Collaborative Intrusion Detection,” *Future Generation Computer Systems*, vol. 135, pp. 30–43, Oct. 2022, doi: 10.1016/j.future.2022.04.028.

[23] M. Bromiley, “Threat Intelligence : What It Is , and How to Use It E ff ectively,” no. September, 2016.

[24] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, “A comparative analysis of cyber-threat intelligence sources, formats and languages,” *Electronics (Switzerland)*, vol. 9, no. 5, 2020, doi: 10.3390/electronics9050824.

[25] W. Tounsi and H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks,” *Comput Secur*, vol. 72, pp. 212–233, 2018, doi: 10.1016/j.cose.2017.09.001.

[26] D. Chismon and M. Ruks, “Threat Intelligence: Collecting, Analysing, Evaluating,” *Cert-Uk*, p. 36, 2015, [Online]. Available: https://www.cpni.gov.uk/Documents/Publications/2015/23-March-2015-MWR_Threat_Intelligence_whitepaper-2015.pdf

[27] E. Miranda Lopez, “A Framework to Establish aThreat Intelligence Program,” p. 73, 2021.

[28] M. B. Jon Friedman, *Definitive guide to cyber threat intelligence: Using knowledge about adversaries to win the war against targeted attacks*. 2016.

[29] M. Phythian, “Understanding the Intelligence Cycle (Studies in Intelligence),” 2013.

[30] D. R. Arikkat *et al.*, “SeCTIS: A Framework to Secure CTI Sharing,” Jun. 2024, [Online]. Available: http://arxiv.org/abs/2406.14102

[31] Daniel. Ish, Jared. Ettinger, and Christopher. Ferris, *Evaluating the effectiveness of artificial intelligence systems in intelligence analysis*. RAND Corporation, 2021.

[32] M. Sahrom, S. R. Selamat, and Y. Robiah, “An Enhancement of Cyber Threat Intelligence Framework Comparative Study of Cyber Threat Intelligence Framework,” 2018. [Online]. Available: https://www.researchgate.net/publication/334697012

[33] G. J. Z. Y. S. X. Yunxue Yang, *Incentive contract for cybersecurity information sharing considering monitoring signals*. IEEE Computer Society, Conference Publishing Services, 2019.

[34] A. Pala and J. Zhuang, “Information sharing in cybersecurity: A review,” *Decision Analysis*, vol. 16, no. 3, pp. 172–196, 2019, doi: 10.1287/deca.2018.0387.

[35] C. Johnson and D. Waltermire, “NIST Special Publication 800-150 (Draft) Guide to Cyber Threat Information Sharing,” vol. 150, p. 73, 2014.

[36] D. E. Zheng and J. A. Lewis, “Cyber Threat Information Sharing,” no. March, 2015.

[37] S. E. Jasper, “U.S. Cyber Threat Intelligence Sharing Frameworks,” *International Journal of Intelligence and CounterIntelligence*, vol. 30, no. 1, pp. 53–65, Jan. 2017, doi: 10.1080/08850607.2016.1230701.

[38] S. E. Jasper, “U.S. Cyber Threat Intelligence Sharing Frameworks,” *International Journal of Intelligence and CounterIntelligence*, vol. 30, no. 1, pp. 53–65, 2017, doi: 10.1080/08850607.2016.1230701.

[39] W. Jurri, “Collaborative Cyber Security in the Retail Sector A collaborative approach to mitigating cyber security risks in the retail sector,” 2014.

[40] W. Tounsi and H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks,” *Comput Secur*, vol. 72, pp. 212–233, 2018, doi: 10.1016/j.cose.2017.09.001.

[41] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*. 2018.

[42] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*. 2018. [Online]. Available: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

[43] S. Barnum, “Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™),” *MITRE Corporation, July*, pp. 1–20, 2014, [Online]. Available: http://blackberry8520.b277.doihaveamobilestrategy.com/http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0_(Draft).pdf

[44] P. Kampanakis, “Security automation and threat information-sharing options,” *IEEE Secur Priv*, vol. 12, no. 5, pp. 42–51, 2014, doi: 10.1109/MSP.2014.99.

[45] MITRE, “Trusted Automated eXchange of Indicator Information — TAXII Enabling Cyber Threat Information Exchange”.

[46] P. Kampanakis, “Security automation and threat information-sharing options,” *IEEE Secur Priv*, vol. 12, no. 5, pp. 42–51, 2014, doi: 10.1109/MSP.2014.99.

[47] N. N. P. Mkuzangwe and Z. C. Khan, “Cyber-Threat Information-Sharing Standards: A Review of Evaluation Literature,” *The African Journal of Information and Communication*, no. 25, pp. 1–12, 2020, doi: 10.23962/10539/29191.

[48] S. Barnum, “Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™),” *MITRE Corporation, July*, pp. 1–20, 2014.

[49] N. N. P. Mkuzangwe and Z. C. Khan, “Cyber-Threat Information-Sharing Standards: A Review of Evaluation Literature,” *The African Journal of Information and Communication*, no. 25, 2020, doi: 10.23962/10539/29191.

[50] M. Mutemwa, “Developing a Cyber Threat Intelligence sharing platform for South African Organisations,” 2020.

[51] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions,” *Comput Secur*, vol. 87, p. 101589, 2019, doi: 10.1016/j.cose.2019.101589.

[52] F. Skopik, G. Settanni, and R. Fiedler, “A problem shared is a problem halved : A survey on the dimensions of collective cyber defense through security information sharing,” *Comput Secur*, vol. 60, pp. 154–176, 2016, doi: 10.1016/j.cose.2016.04.003.

[53] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, “MISP - The design and implementation of a collaborative threat intelligence sharing platform,” in *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, Association for Computing Machinery, Inc, Oct. 2016, pp. 49–56. doi: 10.1145/2994539.2994542.

[54] Nist, “Framework for Improving Critical Infrastructure Cybersecurity,” 2014.

[55] H. Gascon, B. Grobauer, T. Schreck, L. Rist, D. Arp, and K. Rieck, “Mining attributed graphs for threat intelligence,” in *CODASPY 2017 - Proceedings of the 7th ACM Conference on Data and Application Security and Privacy*, Association for Computing Machinery, Inc, Mar. 2017, pp. 15–22. doi: 10.1145/3029806.3029811.

[56] P. Poputa-Clean, “Automated Defense Using Threat Intelligence to Augment Security,” 2015. [Online]. Available: http://www.giac.org/registration/gcih

[57] Homeland Security, “Critical Infrastructure Threat Information Sharing Framework A Reference Guide for the Critical Infrastructure Community,” 2016.

[58] MISP-Contributors, *User guide of misp malware information sharing platform, a threat sharing platform*. 2016. Accessed: Apr. 30, 2024. [Online]. Available: https://www.circl.lu/doc/misp/book.pdf, 2016.

[59] W. Alkalabi, L. Simpson, and H. Morarji, “Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Feb. 2021. doi: 10.1145/3437378.3437391.

[60] F. Skopik, M. Wurzenberger, G. Settanni, and R. Fiedler, “Establishing National Cyber Situational Awareness through Incident Information Clustering,” 2015. [Online]. Available: https://cve.mitre.org

[61] World Economic Forum, “Cyber Information Sharing: Building Collective Security,” 2020.

[62] International Telecommunication Union (ITU), “Guide to Developing a National Cybersecurity Strategy 2nd Edition Strategic Engagement in Cybersecurity,” 2021.

[63] ISO/IEC 27010, “Information technology-Security techniques-Information security management for inter-sector and inter-organizational communications,” 2015. [Online]. Available: www.iso.org

[64] ENISA, “NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies,” 2016, doi: 10.2824/48036.

[65] H. Government, “National Cyber Security Strategy 2016-2021,” 2016.

[66] F. Aferudin and K. Ramli, “The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia,” *Budapest International Research and Critics Institute (BIRCI-Journal)*, 2022, doi: 10.33258/birci.v5i3.6297.

[67] Tewodros Getaneh, “CYBER SECURITY PRACTICES AND CHALLENGES AT SELECTED CRITICAL INFRASTRUCTURES IN ETHIOPIA: TOWARDS TAILORING CYBER SECURITY FRAMEWORK,” 2018.

[68] H. H. Abraha and H. Hailu, “THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA-MAY 2015,” 2015. [Online]. Available: http://www.internetlivestats.com/

[69] W. Zhao and G. White, “A collaborative information sharing framework for community cyber security,” *2012 IEEE International Conference on Technologies for Homeland Security, HST 2012*, pp. 457–462, 2012, doi: 10.1109/THS.2012.6459892.

[70] W. Jurri, “Collaborative Cyber Security in the Retail Sector A collaborative approach to mitigating cyber security risks in the retail sector,” 2014, [Online]. Available: http://essay.utwente.nl/66148/1/Wagenaar_MA_EEMCS.pdf

[71] D. Fernández Vázquez, O. P. Acosta, C. Spirito, S. Brown, and E. Reid, “Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships,” 2012.

[72] S. Isniah, H. Hardi Purba, and F. Debora, “Plan do check action (PDCA) method: literature review and research issues,” *Jurnal Sistem dan Manajemen Industri*, vol. 4, no. 1, pp. 72–81, Jul. 2020, doi: 10.30656/jsmi.v4i1.2186.

[73] V. Braun and V. Clarke, “Using thematic analysis in psychology.”

[74] S. Rahi, “Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development,” *International Journal of Economics & Management Sciences*, vol. 06, no. 02, 2017, doi: 10.4172/2162-6359.1000403.

[75] J. W. . Creswell, *Research design : qualitative, quantitative, and mixed methods approaches*. Sage, 2009.

[76] H. Noble and J. Smith, “Issues of validity and reliability in qualitative research,” 2015, *BMJ Publishing Group*. doi: 10.1136/eb-2015-102054.

[77] INSA, “Critical Mass Cyber Security Requirement Standard Version 2.0.”

[78] INSA, “ፌደራል ነጋሪት ጋዜጣ FEDERAL NEGARIT GAZETTE OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ የሕዝብ ተወካዮች ምክር ቤት ጠባቂነት የወጣ.”

[79] INSA, “የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ ሀገራዊ የሳይበር ደህንነት ፖሊሲ.”

[80] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions,” *Comput Secur*, vol. 87, Nov. 2019, doi: 10.1016/j.cose.2019.101589.

[81] J. En Wagenaar, “Collaborative Cyber Security in the Retail Sector A collaborative approach to mitigating cyber security risks in the retail sector,” 2014.

[82] M. H. Fleming and E. Goldstein, “Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts,” 2012. [Online]. Available: http://ssrn.com/abstract=2201033

[83] S. K. Ahmed, “The pillars of trustworthiness in qualitative research,” *Journal of Medicine, Surgery, and Public Health*, vol. 2, p. 100051, Apr. 2024, doi: 10.1016/j.glmedi.2024.100051.

APPENDICES

Appendix A: Letter of Request

AAiT
Addis Ababa Institute of Technology
አዲስ አበባ ቴክኖሎጂ ኢንስቲትዩት
Addis Ababa University
አዲስ አበባ ዩኒቨርሲቲ

ኢንፎርሜሽን ቴክኖሎጂና ኢንጂነሪንግ ትምህርት ቤት
School of Information Technology and Engineering (SITE)
Elefelious Getachew Belay (Ph.D)

Dean, School of Information Technology and Engineering

ቴሌ Tel: +251-111260194
ፋክስ Fax: +251-(0)11-123-9480
ኢሜይል E-Mail:
elefelious.getachew@aau.edu.et
ቀን፡ ነሐሴ 10/2016
Date: August 16, 2024
ቁጥር Ref No: SITE/1179/16

To: Ministry of Innovation and Technology
Addis Ababa

Subject: Request for Research Input and Data Collection

I am writing on behalf of Addis Ababa Institute of Technology. We are currently running Masters and PhD programs in collaboration with the Information Network Security Administration (INSA) that aims to advance knowledge and research in the field of cyber security.

As part of this program, one of our students, Mihiretu Desalegn Degaga, ID [GSR/0094/13], is conducting research for his thesis entitled "Collaborative Cyber Threat Information Sharing Framework for Collective Cyber Defense in Ethiopia". The study aims to explore critical aspects of cyber security and requires input and data collection from reputable organizations such as yours.

We kindly request your assistance in providing the necessary information to support this important research. Please be assured that any data provided will be used solely for research and educational purposes. The confidentiality of the information will be strictly maintained, and it will not be shared with any third parties.

If you require further information or have any questions regarding this request, please do not hesitate to contact us. We appreciate your cooperation and support in advancing academic research.

Thank you for your time and consideration.

Sincerely,

Elefelious Getachew Belay (Ph.D)
Dean

Addis Ababa Institute of Technology | King George VI Street | Addis Ababa | Ethiopia | P.O.Box 385
Tel. 011-12 32 435 | FAX.011-12 39 480 | info@aait.edu.et | w.aait.edu.et

AAiT
Addis Ababa Institute of Technology
አዲስ አበባ ቴክኖሎጂ ኢንስቲትዩት
Addis Ababa University
አዲስ አበባ ዩኒቨርሲቲ

ኢንፎርሜሽን ቴክኖሎጂና ኢንጂነሪንግ ትምህርት ቤት
School of Information Technology and Engineering (SITE)
Elefelious Getachew Belay (Ph.D)

Dean, School of Information Technology and Engineering

ቴሌ Tel: +251-111260194
ፋክስ Fax: +251-(0)11-123-9480
ኢሜይል E-Mail:
elefelious.getachew@aau.edu.et
ቀን፡ ነሐሴ 10/2016
Date: August 16, 2024
ቁጥር Ref No: SiTE/1175/16

To: Ethio Telecom
Addis Ababa

Subject: Request for Research Input and Data Collection

I am writing on behalf of Addis Ababa Institute of Technology. We are currently running Masters and PhD programs in collaboration with the Information Network Security Administration (INSA) that aims to advance knowledge and research in the field of cyber security.

As part of this program, one of our students, Mihiretu Desalegn Degaga, ID [GSR/0094/13], is conducting research for his thesis entitled "Collaborative Cyber Threat Information Sharing Framework for Collective Cyber Defense in Ethiopia". The study aims to explore critical aspects of cyber security and requires input and data collection from reputable organizations such as yours.

We kindly request your assistance in providing the necessary information to support this important research. Please be assured that any data provided will be used solely for research and educational purposes. The confidentiality of the information will be strictly maintained, and it will not be shared with any third parties.

If you require further information or have any questions regarding this request, please do not hesitate to contact us. We appreciate your cooperation and support in advancing academic research.

Thank you for your time and consideration.

Sincerely,

Elefelious Getachew Belay (Ph.D)
Dean

AAiT
Addis Ababa Institute of Technology
አዲስ አበባ ቴክኖሎጂ ኢንስቲትዩት
Addis Ababa University
አዲስ አበባ ዩኒቨርሲቲ

ኢንፎርሜሽን ቴክኖሎጂና ኢንጂነሪንግ ትምህርት ቤት
School of Information Technology and Engineering (SITE)
Elefelious Getachew Belay (Ph.D)
Dean, School of Information Technology and Engineering
ቴሌ Tel: +251-111260194
ፋክስ Fax: +251-(0)11-123-9480
ኢሜይል E-Mail:
elefelious.getachew@aau.edu.et

ቀን፡ ነሐሴ 10/2016
Date: August 16, 2024
ቁጥር Ref No: SiTE/ 1172/16

To: Information Network Security Administration
Addis Ababa

Subject: Request for Research Input and Data Collection

I am writing on behalf of Addis Ababa Institute of Technology. We are currently running Masters and PhD programs in collaboration with the Information Network Security Administration (INSA) that aims to advance knowledge and research in the field of cyber security.

As part of this program, one of our students, Mihiretu Desalegn Degaga, ID [GSR/0094/13], is conducting research for his thesis entitled "Collaborative Cyber Threat Information Sharing Framework for Collective Cyber Defense in Ethiopia". The study aims to explore critical aspects of cyber security and requires input and data collection from reputable organizations such as yours.

We kindly request your assistance in providing the necessary information to support this important research. Please be assured that any data provided will be used solely for research and educational purposes. The confidentiality of the information will be strictly maintained, and it will not be shared with any third parties.

If you require further information or have any questions regarding this request, please do not hesitate to contact us. We appreciate your cooperation and support in advancing academic research.

Thank you for your time and consideration.

Sincerely,

Elefelious Getachew Belay (P
Dean

School of Information Technology and Engineering (SITE)
Addis Ababa University
Addis Ababa Institute of Technology

Appendix B: Interview Questions

Interview Questions (Type 1)

Information

Name: _____

Age: _____

Sex: _____

Organization: ___

Designation/Role: _____

Years of Experience in Cyber security: _____

Current State

1. Is there presently a framework regulating the sharing of cyber threat information among stakeholders in Ethiopia?
2. What methods are being used for sharing cyber threat information with stakeholders? (such as email, phone communication, online platforms, or other means)
3. What are the sharing standards currently being used for sharing cyber threat information by INSA?

Awareness and Training

4. Have awareness and training programs or campaigns been provided for stakeholders particularly regarding the sharing of cyber threat information? Could you name a few, please?
5. How aware are the public and organizations with the idea of sharing cyber threat information with INSA and among each other (Sector to Sector or organization to organization)?

Legal and Regulatory

6. Can you mention the current legal and regulatory landscape (laws, regulations, frameworks) concerning the cyber threat information sharing in Ethiopia?
7. What role can government (INSA) play in facilitating cyber threat information sharing?

Challenges

8. What are the current main challenges regarding cyber threat information sharing in Ethiopia?

Trust

9. What is your opinion on the existing level of trust among organizations to share cyber threat information?

Collaboration

10. How does INSA collaborate with sector-based SOCs or organizational SOCs in terms of cyber threat information sharing?

Recommendations

What measures or improvements can be made to enhance collaboration and coordination among stakeholders for effective threat information sharing?

Interview Questions (Type 2)

Information

Name: ____

Age: _____

Sex: _____

Organization: _____

Designation/Role: __

Years of Experience in Cyber security: ___

Current State

1. Is there presently a framework regulating the sharing of cyber threat information among stakeholders in Ethiopia?
2. If your organization has prior experience in sharing cyber threat information with INSA or other peer organizations, what sharing **methods** have been used (such as email, phone communication, secure online platforms, or other means), **how frequently** is this information shared **(**weekly, monthly or rarely**)**?

Challenges

3. What challenges exist in sharing cyber threat information? (with INSA, other organizations)

Trust

4. What is your opinion on the existing level of trust among organizations when it comes to sharing cyber threat information (with each other or national regulatory)?
5. What factors do you think influence trust in sharing cyber threat information among organizations?

Collaboration

6. Can you mention some partnership agreements (MOUs) to share cyber threat information with other organizations? (with organizations in your sector and with national cyber security regulator)
7. How do you think information sharing about cyber threats could be improved within your sector and with INSA?

Legal and Regulatory

8. What is your opinion on the current legal and regulatory landscape concerning the sharing cyber threat information in Ethiopia?
9. What role can government (INSA) play in facilitating cyber threat information sharing?

Awareness and Training

10. Have you (your organization) participated in training and awareness programs regarding sharing cyber threat information? Could you name a few, please?

Recommendations

11. What improvements would you suggest for the current cyber threat information sharing practice?

Appendix C: Adopted NIST CSF Categories for the Proposed Framework

Functions	Categories	Subcategory	Description
Identify	Asset Management	ID.AM-3	Organizational communication and data flows are mapped
		ID.AM-5	Data are prioritized based on their classification, criticality, and business value
	Risk Assessment	ID.RA	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management (ID.RM)	ID.RM	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
	Business Environment (ID.BE)	ID.BE-1	The organization's role in the supply chain is identified and communicated
		ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
	Governance (ID.GV)	ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners.
		ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
Protect	Access Control (PR.AC)	PR.AC-1	Identities and credentials are managed for authorized devices and users
		PR.AC-3	Remote access is managed
		PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties
	Awareness and Training	PR.AT	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS)	PR.DS-1	Data-at-rest is protected
		PR.DS-2	Data-in-transit is protected
	Information Protection Processes & Procedures	PR.IP-7	Protection processes are continuously improved
		PR.IP-8	Effectiveness of protection technologies is shared
Detect	Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods.

		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.
	Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties.
		DE.DP-5	Detection processes are continuously improved.
Respond	Communications	RS.CO-3	Information is shared consistent with response plans.
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans.
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Recover	Communications	RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams

Table 9: Mapped NST CSF Subcategories for the proposed framework

Appendix D: Adopted NIST CSF Categories for the Collaboration Process

Collaboration Processes	**NIST CSF Subcategories**	**Description**
Planning	ID.AM-3	Organizational communication and data flows are mapped
	ID.BE-1	The organization's role in the supply chain is identified and communicated
	ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated
	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
Collection	ID.RA-2	This subcategory focuses on developing an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It focuses on receiving cyber threat intelligence information from information sharing forums and sources. The collaboration approach does not only include passively receiving information but also actively contributing to the participating community. This two-way information sharing promotes collective knowledge and defense capabilities across the stakeholders.
	ID.RA-3	This subcategory focuses on the documentation of identified threats. Documentation of threats in one organization is important to create a

		knowledge base that can be helpful to other organizations facing similar challenges.
Analysis	DE.AE-2	This subcategory focuses on the need of organizations in identifying and analyzing potential anomalies and events that may potentially indicate cyber threats. This is by monitoring for compromises on the network or system proactively. In the context of cyber threat intelligence information sharing DE.AE-2 promotes collaborative approach that involves the sharing of detected events and anomalies with collaborating organizations and obtaining detected events and anomalies in return. This will enrich the detection and response capabilities of organizations that engage in cyber threat information sharing ecosystem.
	DE.AE-3	The focus of this subcategory is analysis and mitigation of identified cybersecurity incidents data from multiple sources. This assessment helps to understand the nature and impact of those incidents and to devise suitable response strategies. Regarding sharing cyber threat information DE.AE-3 promotes collaboration of organizations to share the analysis results and mitigation strategies with stakeholders.
	ID.AM-5	This involves the classification of CTI to define a standardized taxonomy for organizing and categorizing to promote effective search, retrieval, and correlation of threat information across the sharing community. The cyber threat intelligence information managed to be shared with the sharing standards such as STIX and TAXII can be given a security classification using Traffic Light Protocol (TLP). The TLP classification is done according to the sensitivity and potential impact that could result from the disclosure of the information.
Sharing	DE.DP-4	This subcategory emphasizes the importance of communicating event detection information shared with other appropriate organizations in order to solve similar vulnerabilities quickly. By sharing this knowledge,

		organizations can collectively improve their ability to identify and respond to cyber threats by leveraging diverse data sources and analysis methods.
	RS.CO-3	This subcategory focuses on cyber threat information shared consistent with the response plans. It emphasizes the importance of sharing information with appropriate stakeholders as part of the incident response process.
	RS.CO-4	This subcategory emphasizes the importance of coordination with stakeholders and ensures the collaboration occurs in line with response plans. It involves the participation of external entities such as sectorial SOC's, government agencies, and trusted partners to collaborate on incident response activities. The participation of external parties enhances the incident response capabilities and results in effective cyber threat information sharing, response coordination, and collective defense against cyber-attacks.
	RS.CO-5	This subcategory focuses on voluntary cyber threat information sharing with to enhance cybersecurity situational awareness. It encourages organizations to participate in information sharing initiatives, both within their sector and across different sectors. This will enhance incident response capabilities of the organizations and contribute to the overall cybersecurity posture on the threat sharing community.
	RC.CO-3	This subcategory emphasizes the importance of communicating recovery activities from a cybersecurity incident to all relevant internal and external stakeholders. Effective communication regarding recovery activities will help organizations to better understand the impact of incidents on their business operations, help to coordinate efforts for effective recovery, and minimize potential impact on organizations business.
Feedback and Continuous Improvement	PR.IP-7	This subcategory concerns the continuous improvement of protection processes through information sharing and coordination. Organizations can learn from incidents that have occurred in other organizations by applying those lessons for the improvement of their own protection processes. By examining and analyzing incidents that have impacted others, threat

		information sharing communities can gain valuable insights into emerging risks, attack vectors, and vulnerabilities. This is a proactive approach that enables organizations to identify potential risks that they haven't encountered yet but that could pose potential threats in the future. By sharing such threat information and collaborating with other stakeholders, they can collectively strengthen their cyber threat protection processes and better defend against advancing cyber threats.
	DE.DP-5	This subcategory describes continuous improvement of detection processes through information sharing and collaboration. By learning from incidents that happened at other organizations and vice versa, organizations can improve their effectiveness of detection processes. The detection and response strategy applied on the incidents at one organization is important to identify gaps, vulnerabilities, and potential weaknesses of the detection processes at another organization. Learning from incidents that have happened elsewhere provides valuable insights into new attack techniques, indicators of compromise (IoCs), and emerging threat patterns. This knowledge can inform the refinement and enhancement of detection processes, enabling organizations to proactively detect and respond to similar threats happened already on other organizations within the cyber threat sharing ecosystem.

Table 10: Subcategories mapped for the collaboration process

Appendix D: Adopted NIST CSF Categories for the Collaboration Governance

Collaboration Governance	NIST CSF Subcategories	Description
Role and responsibilities	ID.BE-1	The organization's role in the supply chain is identified and communicated
	ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated
	ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
Awareness and Training	PR.AT	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information

		security-related duties and responsibilities consistent with related policies, procedures, and agreements.
Legal and Regulatory Compliance	ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
Data Privacy and Security	PR.AC-1	Identities and credentials are managed for authorized devices and users
	PR.AC-3	Remote access is managed
	PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties
	PR.DS-1	Data-at-rest is protected
	PR.DS-2	Data-in-transit is protected
Risk Assessment and management	ID.RA	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	ID.RM	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Table 11: NIST CSF subcategories mapped for the collaboration governance layer