TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

Abenezer Berhanu Weldegiorgis IVCM177244

DEVELOPING NATIONAL CYBERSECURITY STRATEGY FOR ETHIOPIA

Master's Thesis

Supervisor: Mika Kerttunen(D.Soc.Sc)
Senior Research Scientist

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tarkvarateaduse instituut

Abenezer Berhanu Weldegiorgis IVCM177244

ETTEPANEKUD ETIOOPIA KÜBERTURVALISUSE STRATEEGIA JAOKS

Magistritöö

Juhendaja: Mika Kerttunen(D.Soc.Sc)
Vanemteadur

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Abenezer Berhanu Weldegiorgis

13.05.2019

Abstract

With the global nature of cybercrime and the importance of cyberspace for country development, it's crucial for countries to develop and implement a cybersecurity strategy not only at an organizational level but also at a national level.

International frameworks and standard guidelines have been put in place to help national leaders and policymakers to develop national cybersecurity strategy; however, with the uniqueness of any national realities, these approaches have to be tailored with countries national ambition, resource, and priority areas.

So far many countries have developed and implemented national cybersecurity, or information security strategy. Ethiopia as headquarter of the African Union and with a future potential of becoming a center for digital transformation in the region needs an effective national level strategic document in the area of cybersecurity.

Based on the analysis of the domestic ICT environment, international guidance, other countries best practices, and knowledge gained from subject matter experts, this paper proposes guidelines for Ethiopia National Cybersecurity Strategy.

The main argument of this study is national cybersecurity strategy is a useful tool to solve cybersecurity problems at a national level, and countries can learn from other countries and available international guidance, to develop and implement a flexible and dynamic national cybersecurity strategy, hence these approaches should be tailored with the national ambition, resource and priority areas.

This study can be used by the government and policy makers in Ethiopia to design and develop National Cybersecurity Strategy and as a knowledge base for future research on the area. This thesis is written in English and is 54 pages long, including six chapters, nine figures, and eight tables.

Keywords: Cybersecurity, Strategy, Guidelines, Cybercrime, Cyberspace.

Acknowledgments

First and foremost I would like to thank almighty God for his countless love and protection throughout my life. My sincere gratitude goes to my supervisor Mika Kerttunen (D.Soc.Sc) for his invaluable advice and guidance throughout this research.

I would also like to thank the experts who were involved in the interview and the online questionnaire for this research. Finally, my deepest gratitude goes to my family and friends for their encouragement and support throughout my years of study.

List of abbreviations and terms

AU	African Union
CCDCOE	Cooperative Cyber Defence Center of Excellence
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
COMESA	Common Market for Eastern and Southern Africa
CTO	Commonwealth Telecom Organisation
ECOWAS	Economic Community of West African States
EFTA	European Free Trade Association
ENISA	European Union Agency for Network and Information Security
EU	European Union
FDRE	Federal Democratic Republic of Ethiopia
FBI	Federal Bureau of Investigation
G8	Group of Eight
GPD	Global Partners Digital
GTP	Growth and Transformation Plan
ICT	Information and Communication Technology
INSA	Information Network Security Agency
ITU	International Telecommunication Union
IBM	International Business Machines Corporation
IT	Information Technology
ISO	International Organization for Standard
NCSS	National Cyber Security Strategy
NCSFM	National Cyber Security Framework Manual
NATO	North Atlantic Treaty Organization
NCSI	National Cyber Security Index
NCAP	National Cybercrime Action Plan
NIST	National Institute of Standards and technologies
NISP	National Information Security Policy

PDPA	Personal Data Protection Act
R&D	Research and Development
SADC	Southern African Development Community
UN	United Nations
USD	United States Dollar
RQ	Research Question

Table of contents

List of figures

List of tables

1 Introduction

The internet and the growing extension of integrated information systems to almost all aspect of trade and governance has brought an excellent advantage for society by creating opportunities and services which results in remarkable achievements. These days information and communication systems are involved in almost in all aspect of our daily life, and also has triggered countries to get involved in the digital age [1].

Nonetheless, the increasing extension of connected information systems and the growth in the speed, convenience, and anonymity of the internet has paved the way for a variety of potential cyber threats know to have no physical or virtual boundaries, making countries more vulnerable to cyber-attacks.

In the past few decades, many cyber-attacks had occurred, one of the significant large-scale cyber-attack occurred on April 2007, against Estonia which was claimed to be politically motivated cyber-attack, the attacks posed a considerable threat and drew worldwide attention [2]. This attack showed that cyber-attacks could grow into an extent of threatening national security and triggered a need for a comprehensive NCSS [2].

Overwhelmed by this and growth in cyber-attack all over the world, countries undergo a change in their national cybersecurity landscape, by formulating or amending laws and regulation. The international community has also put much effort to put specific terms and obligations on the cyberspace; however, the growth in cyber threat and its complexity, made policy development very challenging.

The legal, technical and organizational difficulties posed by the cybersecurity are worldwide and are even higher in the developing world, because of the shortage of cybersecurity professionals and technical resources [3].

The challenges can only be addressed through a comprehensive strategy in the context of international cooperation, by considering the role of different vital stakeholders and existing initiatives [4]. A strategy is designed to be tailored with the national context and realities, not of adopting globally accepted measures [5]. Strategies are issued to inform and educate domestic constituencies and foreign audiences, by giving political guidance, setting objectives, selecting priorities, providing resources, legitimizing direction and content of the policy adopted [5].

There are various motivation and approaches for developing NCSS including achieving state's national interest security, initiating government priorities, and economic interest. Because of the existence of a different understanding of security issues, so far there is no universal approach formulated in the world politics in the cyberspace, and nations are attempting to establish side deal compliance assistance in cyberspace [6].

Developing and implementing a cyber-security strategy is as a step forward effort for improving the countries cyber environment; however, the strategy has to be made in such a way that it fits with the country's political, operational, financial and technological context [5]

Besides the various motives and approaches, with the ongoing increase of cyber threats, there is an urgent need for countries to cooperate for fighting against cybercrime [7]. In September 2011 ITU published guideline suggesting countries to develop national cybersecurity strategy with a realization of national cyber risk, which was followed by other guidelines and frameworks recommending nations on what to include on their national cybersecurity strategies, however, "there is no one-size-fits-all security method or tool" [8].

Which shows there is no universal approach, framework, or guideline which fits for all developed and developing nations as a whole. Different factors such as the political, legal, organizational, and national view of cyberspace create a national difference in approaching important issues in NCSS [9].

Therefore, based on analyses of a domestic ICT environment, expert opinion, other countries best practice and international guidance, we propose guidelines for Ethiopian National Cybersecurity Strategy which meets the country national strategic objectives, goals, and priorities.

1.1 Problem Statement

Ethiopia as a developing nation is not left out of the benefits as well as the challenges on the cyberspace. Ethiopia is in the way of integrating ICT into critical infrastructure, as a developing country much effort has been made so far to formulate regulatory institutions and information security policy to combat against cyber-crime.

However, the advancement in technology has resulted in the sophistication of crime commission methods, which makes traditional laws and crime investigation methods out of use. Cyber-attack in the country is growing at a fast rate, the government of Ethiopia enacted the first National Information Security Policy on 2011, and this policy document has been taken as a starting point to move towards minimizing cyber-crime in the country.

The Ethiopia National Information Security Policy of 2011 addresses the need to create a reliable, safe, secure and resilient information environment, which supports the country national vision to alleviate from poverty and become middle-income economy [10].

The developmental state ideology of the government has also led the country to have a closed, and government-controlled economy, where most of the firms including Telecoms, Airlines, Ethiopian Power, and the Maritime Transport are under the state monopoly.

However, as part of the economic reform in 2018, the government of Ethiopia has issued deregulation and privatization of key economy sector by opening the major state-owned firms to private domestic and foreign investment [11]. This reform is going to attract different foreign high tech investment into the country, which is believed to bring a dramatic change to the national cybersecurity environment.

So this economic and social reform needs to be supported by new strategies and policies which can put specific regulations and obligations on the cyberspace. The 2011 National Information Security Policy of Ethiopia helps as a guiding principle or a principle of action, for a different body of the government to make logical decisions, and it is a national-level cybersecurity strategy or equivalent on National cybersecurity index [12].

However, it fails to address the current cybersecurity environment of the country and also it does not provide conditions which ensure an appropriate level of cybersecurity in the country in such a way that by failing to adequately address the notion of critical infrastructure, links with other national and international strategies, public-private partnership, lack of update or review mechanism.

Information security policies, doctrines, and strategies are generally narrower by the scope, and national cybersecurity strategy tends to include critical infrastructure protection, countering cybercrime, international cooperation, national and international issues.

Despite the existence of National Information Security Policy in Ethiopia, there is an apparent lack of a practical, comprehensive strategy that addresses contemporary cybersecurity challenges.

The contemporary country's economic reform and the accompanying ongoing critical projects make the current information Security policy of Ethiopia outdated and trigger a need to create a new comprehensive national cybersecurity strategy which will take consideration of the country national strategic objectives, goals, and priorities.

Therefore based on the analysis of the domestic ICT environment, international guidance, other countries best practices, and knowledge gained from subject matter experts the study proposes guidelines for Ethiopia National Cybersecurity Strategy which is tailored with the national ambition, resource, and priority areas

2 Methodologies

Based on the analysis of the domestic ICT environment, international guidance, other countries best practices, and knowledge gained from subject matter experts, this paper proposes guidelines for Ethiopia National Cybersecurity Strategy which is tailored with the national ambition, resource, and priority areas.

2.1 Research Questions

The key central question is,

RQ1. What strategic directions Ethiopia should follow to develop a more consistent NCSS which is tailored with the country national ambition, resource and priority areas?

Sub-questions:

RQ2. What is the contemporary cybersecurity environment in Ethiopia?

RQ3. What best practices, measures, approaches, and tools can be taken?

2.2 Research Design

In preparing this paper and presenting the outcome, we used several methods starting with an initial review of similarly related research documents, analysis of existing standard guidelines. Followed by an analysis of National Cybersecurity Strategies of Canada, Germany, Singapore, and Rwanda which enable us to get a useful insight of provisions of cybersecurity policy approaches, best practices, measures and observe challenges in the strategy development process.

The selection of countries was made based on the level of resemblance with Ethiopia in terms of strategic interest, government ideology or high rank in the National Cyber Security Index. Then after, an online questionnaire was distributed anonymously using Google survey form. The online questionnaire contains 20 questions and data was collected from public and private organizations in Ethiopia to gain an overview of the contemporary cybersecurity environment and challenges in the country.

Afterward, semi-structured interview was conducted to collect data from subject matter experts in the area of National cybersecurity strategy which enabled us to identify and get an understanding of the ongoing debates, topics, and problems on the area.

Finally, we proposed guidelines for Ethiopia National Cybersecurity Strategy which is tailored with the national ambition, resource, and priority areas. Whereas, because of model results are always nonunique, and natural systems are never closed the validation of models of natural system is not possible;and, models, can only be confirmed in accordance with observation and prediction, and also a complete confirmation is logically prohibited, though models can be evaluated with respect to terms and their predictive value. [13].

2.2.1 Limitations and key assumptions of the study

The research is limited to the information which was made public and available to everyone.

Key Assumptions:

- National cybersecurity strategy is a useful tool to solve cybersecurity problems at a national level. Countries can learn from other countries and available international guidance, to develop and implement a flexible and dynamic national cybersecurity strategy, and these approaches should be tailored with the national ambition, resource and priority areas.

2.3 Data Collection

For data collection an online questionnaire was used as a survey instrument followed by semi-structured interview; the survey was conducted from February 5, 2019, to March 3, 2019. To ensure the validity of these instruments, the instruments were developed by taking account of previously conducted studies on cybersecurity [14] [15].

The online questionnaire was prepared by using google questionnaire form and sent to public and private organizations in Ethiopia, and 30 response was collected.

For this study five experts in the area of national cybersecurity strategy development, law, and policy making were interviewed, the interview lasted from 30 minutes to an hour.

The interview included two experts from Ethiopia which are in charge of cybersecurity policymaking and execution, and three foreign experts and researchers from Estonia, Germany, and Nigeria. Different channels were used to conduct the interview. Four of the interview was conducted through electronic medium Skype, whereas one is conducted face to face.

3 Literature Review

This section will address academic knowledge and experts views concerning National Cyber Security Strategy development by analyzing the challenges in the absence of common agreed definitions and different approaches for developing NCSS.

The section also analyzes the existing cybersecurity environment in Ethiopia and legal frameworks which gives a basis for our study followed by an analysis of other countries best practices, measures, and approaches to developed NCSS, finally, we will give an overview of international and regional conventions on cybercrime, as well as existing frameworks and practical guidelines.

3.1 Ethiopia and the Digital Landscape

Even though Ethiopia is lagging in ICT in contrast to other developing countries, ICT penetration in Ethiopia is steadily growing [15]. According to Digital in 2018 Global Overview Report, Ethiopia with over 106.2 million total population, internet penetration rate of the Ethiopia is 15 %, and there are 16.4 million internet users in the country, out of those 3.8 million are active social media users with a penetration rate of 4% as well as over 53.3 million mobile connection users which constitutes 50% of the total population [16].

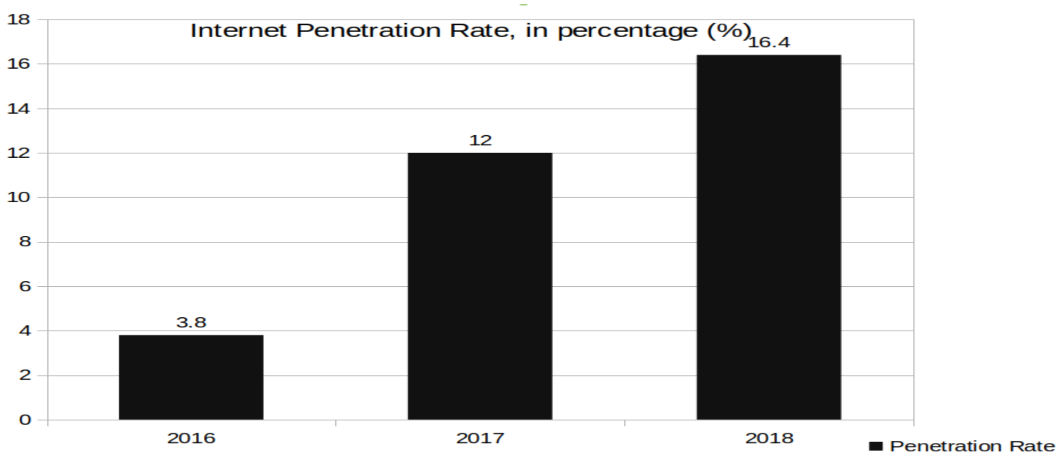


Figure 1 Internet penetration rate Source

As we can observe from the graph, the internet utilization in the country is low but steadily growing, due to a significant user base potential and the ongoing growth on ICT infrastructure in Ethiopia there exists a high probability that soon the country can be ICT hub of Africa.

The vast expansion of ICT infrastructure in the country led to increasing usage of internet in the country, in 2010 Ethiopian government formulate the first five years growth and transformation plan(GTP I) which cover the years 2010/11-2014/15 [17].

As part of GTP I, the expansion and quality of infrastructure was given priority, and huge investments were made by the government to acquire new technologies and services [15]. As a result of this effort, the usages of ICT services has increased, the number of telecom service users grows from 7.7 million in 2009/10 to 39.8 million by 2014/15, within the same period of time the number of mobile subscribers increased from 6.7 million in 2009/10 to 38.8 million by 2014/15, and the significant achievement was the introduction of 3G and 4G internet networks [18].

The years from 2015/16-2019/20 has also been covered on the second growth and transformation plan(GTP II), within this period of time the government planned to grow mobile usage and telecom density from 43.9% to 100%, and 10.5% to 54% respectively, whereas increase internet and international link capacity from 3.3% to 10% and from 27.9Gbs to 1485Gbs respectively by maintaining mobile coverage at its current level which is around 81% [18].

In 2010 Ethiopian government has also adopted e-government strategy and several agencies are currently giving services through a government portal. The country cybersecurity response can be observed concerning policies, strategies, legislation, and institutional arrangements.

3.2 Cybercrime in Ethiopia

According to reports the security situation of Ethiopia and the entire horn of Africa is very tense, and there exists a highly volatile geopolitical intersection [19].

The political unrest in Ethiopia was accompanied by major cyber-attacks, including hacktivism and fake news. Reports show that within only six months of 2016/2017 Ethiopia was hit by more than 256 cyber-attacks including the recent WannaCry ransomware [20].

The former Prime Minister of Ethiopia stated on the United Nations general assembly that "Social media has empowered populists and other extremists to exploit people's genuine concerns and spread their message of hate and bigotry without any inhibition" [21]. On his word, he indicated the frustration of the government on the issue and the social, political and economic consequence it has on the country.

However, according to a report by Citizen Lab the Ethiopian government by itself has been accused of cyber-attacks targeting political opponents and activists living abroad [22]. Concerning the current reality and existence of cybercrime and to get a clear picture of cybercrime situation in the country, an online questionnaire was distributed, and results were collected from various cybersecurity specialists and information technologies professionals who work in public and private organizations in Ethiopia, analyzed and presented on the study.

Besides the online survey, other sources also show that there is a high rate of cybercrime in Ethiopia, Kaspersky report put Ethiopia as one of the top countries where users face the highest risk of local malware infection and one of the most malware-infected country in the world [23].

The government has been taking different measures to fight against cybercrimes, which includes the National Information Security Policy in 2011. Which lays the ground for different laws including legislation on e-commerce, e-signature, cybercrime, and telecom fraud proclamations, and the more recent Critical Mass Cybersecurity requirement standard of 2018 however as we can understand from the contemporary situation of Ethiopia and the survey result the cybercrime is growing threat in Ethiopia and needs a comprehensive response.

3.3 NCSS Development in Ethiopia

According to ENISA NCSS, Good practice guide, National cybersecurity strategies (NCSS) are fundamental documents of a country which are used to set strategic principles, guidelines, and objectives and in some cases specific measures for mitigating cybersecurity risk [24].

The national view of cyberspace can be understood through an overview of the national cybersecurity situation in the country is described in such a way that enable as to adapt parts of the strategy according to unique national features. This process consists of gathering and analyzing of information from different sources, such as online survey, semi-structured interview, and from various written sources including reports, articles, and magazines.

3.4 Institutional Setup

The national context of cybersecurity in Ethiopia can be presented concerning the usage of ICT infrastructure and ICT-based services; this can be observed through institutions which are responsible for the overall ICT service.

3.4.1 Ministry of Innovation and Information Technology

Previously known as Ministry of Science & Technology and Ministry of Communication and Information Technology, was first established in 1975 as a commission by proclamation No.62/1975 [25].

With regards to a new economic policy by the Federal Democratic Republic of Ethiopia, it was re-established again in March 1991 by directive No.90/94, the next phase of re-establishment was on 24th of August 1995 as an agency later the ministry changed its name to Ministry of Innovation in October 2018 [26].

The agency-specific duties include promoting the growth of ICT services, regulating telecommunication, monitor government domain names and register address, support and conduct research and design, work with educational institutions to promote education in the field of information technology and many other duties [26].

Hence the Ethiopian government gave the agency a comprehensive instruction to advance the growth and development of ICT.

3.4.2 Information Network Security Agency (INSA)

INSA was established by proclamation No.808/2013, and it is the only primary institution in Ethiopia regulating, and handling cybersecurity issues with national security perspective, the agency is accountable to the prime minister and its head office located at the capital city Addis Ababa [27].

The agency duties include drafting national policies, laws, standards, and strategies which enable to:

- Safeguard information and computer-based essential infrastructures security, and oversight their enforcement upon approval;
- Administer national emergency responding center;
- Conduct a forensic investigation; regulate cryptographic products and their transactions;
- Develop and implement secured infrastructures and systems;
- Regulate and control import-export of information technology, information sensor and information attacking technologies [27].

3.4.3 Federal Police Commission

The Federal police commission was established by proclamation No.720/2004 with principles of non-partisanship and power to investigate crimes in Ethiopia [28], the Computer Crime Proclamation No.702/2011 Article 6(5) designate Federal Police Commission to investigate crimes related to information network and computer system [28].

Federal Police Cyber Unit Division was established in 2004 with the support of American FBI cybercrime investigations in the country pass through them, INSA provides technical support and training to the unit, however, there exists a challenge on effectively addressing cybercrime [17].

3.4.4 The National Intelligence and Security Service (NISS)

The NISS is re-established by Proclamation No. 804/2013, and it is accountable for the prime minister with a power to lead the work of intelligence and security services, its duty includes:

1. Fighting against cybercrime both inside and outside the country responsibly;
2. Issue directive and standard for the protection of critical institutions; follow up threats to economic security;
3. Collect necessary data and provide it to the appropriate body [29].

3.5 Legal and Policy Framework in Ethiopia

Within the past few years, Ethiopia has been enacting different pieces of legislation, the first cybercrime-related legislation in Ethiopia enacted in the criminal code of the Federal Democratic Republic of Ethiopia in 2004.

Moreover, other legislation including the Payment System Proclamation [30], the Registration of Vital Events and the Identity Card Proclamation [31] and then National Telecom Fraud Proclamation [32] has also been enacted. In which the National Payment System proclamation regulates the country payment system to ensure a safe, secure, and efficient service especially in bank sectors however the law does not adequately address the cybersecurity issues to electronic payment system except dealing with forgery and fraudulent activities.

The second Proclamation dealt with the issuance of electronic identity card in which there is an ongoing project by the Ethiopian government to implement it in some part of the country. This proclamation addresses cybersecurity issues and emphasized protection of information from attacks or other forms of abuse and the third Proclamation regulates illegal usage of SIM card, credit cards, and data [32].

The most recent legislation towards regulating Cyber Crime was enacted in 2016, as Computer Crime Proclamation No.958/2016 and it has introduced evidentially and a procedural rule which can assist investigation and prosecutions. However, according to [33] this proclamation received criticisms from various corners due to its provisions that potentially conflict with constitutionally guaranteed rights. Based on the discussion the legislation mentioned above and regulatory frameworks in Ethiopia are not adequate, and there is a need for comprehensive cybersecurity laws.

3.5.1 National ICT policy and strategy of 2009

The National ICT policy and strategy of 2009 mainly aimed at establishing an accessible ICT infrastructure, developing skilled human resource, and strengthening the private sectors all over the country [34]. Through public sector and capacity building framework this policy addresses the need for implementing e-governance technology for effective delivery of government services focusing on Government to Government (G2G), Government to Business (G2B), Government to citizen (G2C) and Government to Employee (G2E) service delivery [34].

3.5.2 Ethiopian National Information security policy of 2011

The National Information Security Policy of 2011 is the first cybersecurity policy in Ethiopia; the policy addresses that the country is vulnerable to cybercrimes and the need for minimizing threats and vulnerabilities the policy also addresses ICT with cybersecurity implication in regards to the legal system and security strategy [10].

The policy defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the internet, telecommunication networks, computer systems, and embedded procedures and controllers" [10].

The Information Security Policy is limited to the public sectors, and information security is described in the document as "the integral part of the national security, organizational security, public peace and security, and the protection of basic rights and freedoms of citizens" [10].

The adoption of this policy has led to the establishment of a specialized institution dedicated to safeguarding cybercrime, INSA was established in 2006, and it is the only institution in Ethiopia regulating, and handling cybersecurity issues with a national security perspective.

3.6 Terms and Definitions

One of the major challenges that policymakers face when developing NCSS is the lack of commonly agreed definition for terms such as “cyberspace” and “cybersecurity” this has also created a challenge when states need to cooperate and collaborate [35]. So that it is very important to include and establish a commonly agreed definition on the NCSS [35] [36].

Finding a common standard definition on a global scale for terms is very challenging, however, various countries, institution, and researchers defined these terms in such a way that goes along with their need, understanding, and perspectives [35].

A study at [37]describes the historical background definition of the term “cyberspace” going back to early 1980s as “a graphic representation of data abstracted from banks of every computer in the human system” [37] which emphasize on the basic information security aspects.

With increased usage and expansion of ICT more broader and detailed definitions were later presented, a study at [7] defined the term “cyberspace” with a more border explanation as all actors including people who are directly or indirectly interact with the network [7].

Whereas ITU excludes people and their interaction from the former [7] definition and describes it with a broader range as the direct or indirect interconnection of systems and services with the whole ICT infrastructure [8].

Most countries define or describe cyberspace on their national cybersecurity or information security strategy as the whole network of physical as well as virtual ICT devices [38].

The table below described how some countries used to define the term cyberspace on their strategy.

#	Definitions	Countries
1	Cyberspace as the whole network of physical as well as virtual ICT devices	USA, UK, France, India, Saudi Arabia, and Turkey
2	Cyberspace as it only refers to the “internet” and internet connected ICT devices	Australia, New Zealand, Germany, Spain, and Canada
3	No clear definition provided	Netherlands
4	The term “Cyber domain” has been in use instead of “Cyberspace.”	Finland

Table 1 Cyberspace defined by various countries [38].

Ethiopia also defined Cyberspace on the 2011 Ethiopian National Information Security Policy as “a global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the internet, telecommunication networks, computer systems, and embedded procedures and controllers” [10] which basically follows a comprehensive approach and can be taken as it is on future NCSS development.

Cybersecurity and Information security have been defined and used interchangeably. Besides the usual similar definition and interchangeable usage of the terms, a study [39] spot out the difference among the two terms by defining information security as limited to protection of information asset either it exist in physical or nonphysical form, whereas cybersecurity as an all-inclusive both information and no information assets within the ICT infrastructure [39].

3.7 NCSS Development Approaches and Processes

Despite the effort made by countries and the international community to put specific terms and obligations on the cyberspace, different countries and organizations have tried to stipulate different approaches and frameworks towards developing cybersecurity strategy which is tailored with a specific agenda of the issuer.

The study by Shears, Schnidrig, and Kaspar [40] suggested a multi-stakeholder approach for national cybersecurity strategy development, by taking the four characteristics identified by GPD’s Framework for Multi-stakeholder Cyber Policy Development [40].

The study by Shears, Schnidrig, and Kaspar [40] also defines four essential characteristics of NCSS development; these are open and accessible; inclusive of stakeholders' views; consensus-driven; transparent and accountable.

An insight of relevant stakeholders to be involved in the strategy development process guarantee that the strategy has all the support of the stakeholders [40].

Whereas, Kerttunen [5] identifies a commitment to development approach, by portraying determining factors of national cybersecurity strategy and addressing future possibilities. The study also points out that strategies cannot be pre-ordered but have to be formulated in a way that fit the country's political, operational, financial and technological realities [5].

The study by Kerttunen [5] entails to empower countries to distinguish requirements and abilities, threats and risks also give an insight into potential domestic as well as international cooperation; the study also proposes a development-first strategic approach which perceives and takes account of the national ICT, digital and information security strategy process [5].

Much older studies depict approaches based on theories on addressing cybersecurity problems, which includes national security, economic, and public health theories [3] [41].

The study by Mulligan and Schneider [41] address formulating policy and political agreements as a solution for cybersecurity problems. Mulligan and Schneider [41] also put public cybersecurity doctrines which formulate legal framework as the basis required for making cybersecurity policy an all-inclusive other than individual.

In addition to the above-mentioned approaches and process, different countries, regional and international organization proposed and implemented different approaches and process.

3.8 Analysis of Other Countries Cybersecurity Policies and Strategy

Cybersecurity strategy has become one of the topmost priorities of governments all over the world. For the past few decades, 106 countries have developed and implemented national cybersecurity or information security strategy as well as they are putting an effort to renew, and update their policies; however, many other developing nations are on their initial step of developing a national level cyber security strategy [42].

Here will analyze selected countries national cybersecurity or information security strategies which enable us to get a useful insight of provisions of cybersecurity policy approaches and observe challenges in strategy development process this can also help us to take approaches/models that can be used for our study.

The basis for the selection of countries was according to one of the following consideration:

- States should have a functional cybersecurity strategy/policy, and it should be available online;
- States should have similar enough problems and realities like Ethiopia;
- States cybersecurity ranking index according to ITU [43];
- The countries resemblance to Ethiopia either in terms system of government, government ideology, or political nature;

By examining the cybersecurity policies and strategies of each country, we will extract common essential components/values.

Canada

A strong cybersecurity posture and federal system of government made Canada suitable for this study. In 2010 the government of Canada published NCSS which lays bases for future actions to protect citizens, industry, and government from cyber threat, the strategy defines cyberspace as an electronic world which results from the interconnection of networks [44].

The strategy prompts Critical infrastructure policy by imposing the National Strategy and Action Plan. And it outlines a digital infrastructure protection plan by the Throne, provinces, territories and the private sector [45]. The Canadian NCSS tries to address national security, from a distinct perspective of protecting critical infrastructure, and the strategy is built upon three strengthening pillars:

1. Securing government systems;
2. Partnering to secure vital cyber systems outside the federal government;
3. Helping Canadians to be secure online [44].

Concerning the perceived cyber threats, the strategy mainly aimed at addressing three categories of cyber threats which includes:

- State-sponsored military activities and cyber espionage;
- Internet use by terrorists;
- Cybercrime [46].

The strategy designates clear roles and responsibilities for federal agencies such as Public Safety, Department of National Defence and the Canadian Forces, Royal Canadian Mounted Police and others [46].

The Action Plan for critical infrastructure formulate a collaborative approach between federal, provincial, territorial, and critical sectors and it strengthens the country resilience in critical infrastructure by specifying actions to be taken in the areas of collaboration, risk management and information sharing [46] [47].

Canada established the Cybercrime Fusion center and much other legislation such as Anti-spam legislation and Safeguarding Canadians Personal Information Act on fighting

against cybercrime and also works jointly with the United Kingdom, New Zealand, NATO, G8, and UN agencies to enhance their Cybersecurity capacities [45].

The strategy also permits the continual review and improvement to meet emerging new threats and also address enhancement of cybersecurity awareness partnering with the Provinces and territories, private sectors and critical infrastructure sectors, in overall the strategy mainly bases on addressing the protection of critical national infrastructure [44].

Germany

The Federal form of government and high rank in NCSI makes Germany suitable for our study. Germany published a cybersecurity strategy based on a comprehensive approach. The strategy mainly focuses on civilian approaches and measures which aims at ensuring the consistency and potential of the international community to safeguard the cyberspace [48].

The strategy was first published in 2011 and later updated In November 2016 and made to include more extensive content than the previous [48] [49]. The key strategic focus areas or line of actions includes:

- Protection of critical information infrastructure through public and private sectors coordination;
- Strengthening IT security through creating awareness on risks related to the use of the IT system; Set up National Cyber Response Center for fast and reliable information sharing and cooperation between state authorities on the cyber incident ;
- Enhancing the legal framework and law enforcement agencies for effective crime control also in cyberspace
- Use of reliable information technology through the development of innovative protection plans [48];

In contrast with other nations, German NCSS mentioned threats which may result from the mismatch between growth in functional development of ICT and the country level of cybersecurity readiness to address those threats, while other countries other than Japan do not mention it on their NCSS [50].

Even though it would be challenging to address who is responsible, the NCSS of Germany recognizes global cyberinfrastructure as stakeholder [50]. On the implementation section of the strategy, it is clearly stated the need for a regular review of the document under the control of the National Cybersecurity Council [50].

The German NCSS also gives a more precise definition and lists specific area which is identified as critical infrastructure. And focuses on four areas of action such as safe and independent use of the digital environment; cooperation between the German state and the economic sector in the cyber field; building an effective cybersecurity architecture in the public sector; making Germany a central actor in the European and global cyber policies [48] [49].

Singapore

A strong economy tie with Ethiopia and the resemblance of the developmental state government ideology [51] [52], make Singapore suitable for our study. In 1965, after gaining independence, Singapore followed state-led development in which there is strong government involvement in various key sectors to increase the country's economy [53].

However, recession in 1985 arose the need for deregulation and privatization in the country, and within the next few decades, many critical infrastructures including the telecommunication were given to the private sectors in a varying pace [53].

The privatization of critical infrastructures was substantially different across different sectors with varying level of the public sector ownership/share on the critical infrastructures, which has led to difference on handling cybersecurity across the sectors [53].

Within sectors which are majorly owned by the government or privately owned companies and operators of critical infrastructure, the government intervenes to ensure cybersecurity in the form of legislation enacted at the national level, and regulations implemented at sectoral level [53].

The Singapore Cybersecurity Strategy set out the country vision, goals and priorities for cybersecurity; the strategy addresses security in the cyberspace concerning four pillars :

1. Strengthen the resilience of Critical Information Infrastructures;
2. Mobilize businesses and the community;
3. Develop a vibrant cybersecurity ecosystem;
4. Step up efforts to forge strong international partnerships [54].

The strategy promotes security by design approach in the system development life cycle. Singapore has also developed a national cybersecurity response plan, which aims at the timely responses and initiatives at the local level, supported with successful collaboration and strategic support at the sectoral and national level [54].

The strategy addresses the borderless nature of the cyber threat and promotes the use of the National Cybercrime Action Plan (NCAP) to combat cybercrime with a coordinated effort of the nation, by:

1. Educating the public for a safe in cyberspace;
2. Second, increase the Government's capability to fight against cybercrime;
3. Third, enhance legal frameworks;
4. Finally, step up partnerships and international engagement [54];

The strategy also addresses personal data protection under PDPA and promote education on cybersecurity area [54]. The contemporary situation in Ethiopia have similar enough problem and realities as that of Singapore, Ethiopia with a state-led development ideology like Singapore, is on the way of deregulation and privatization of key economy sector including telecommunication so analyzing challenges and measures that are taken by Singapore on the transition have a great advantage to our study.

Rwanda

In response to the ever-increasing cyber threat and improving cybersecurity for individuals and key economic sectors, the Rwandan government enacted the National Cyber Security Policy in March 2015 [55].

The policy emphasizes and outlines a three-folded approach to cybersecurity which are:

- To increase the level of cybersecurity awareness and protect key ICT assets against attacks.
- To build local capabilities to respond to attacks as well as foster international cooperation on cybersecurity.
- To create a legal and regulatory environment to mitigate cyber vulnerabilities [55].

Rwanda also enacted National Cyber Security Strategic Plan which provides implementation guidance for the National Cyber Security Policy [56].This framework specifies the foundation of different regulatory institutions such as:

- National Cyber Security Advisory Board (NCSA);
- National Cyber Security Agency (NCSA);
- Public and private institutional ICT units with cybersecurity functions and specialized cybersecurity centers [56].

Legal Framework has also been put in place to establish and determine national cybersecurity authority mission, organization and functioning [57].

3.9 International and Regional Conventions on Cybercrime

Regardless of domestic legislation, to adequately address the issue of cybercrime, there needs to be co-operation at the regional and international level [17]. Many efforts have been made so far by different international and regional organizations to enact legislation in cybercrime, one of which is the European Convention on Cybercrime [58] which was at first intended to be a regional convention and later got a full range of acceptance across the globe.

In addition to that, on June 27, 2014, African Union has also adopted a Convention on Cyber Security and Personal Data Protection [59] which meant to tackle cybersecurity challenges that hinder the growth of electronic commerce in Africa. On this section, we will discuss the implication of both the European Convention on Cybercrime and the AU Convention on Cyber Security and Personal Data Protection to the Ethiopian legal system.

3.9.1 Convention on Cybercrime of the Council of Europe (CETS No.185)

The Convention on Cybercrime of the Council of Europe which is known as Budapest Convention was drafted on November 23, 2001, Budapest, Hungary; the convention is the most comprehensive and the first international treaty on combating cybercrime [60]. The convention aims to harmonize domestic laws, give power for domestic criminal procedural law to investigate as well as prosecution of offences and build up strong international co-operation [58].

The significant offences on the Convention are grouped into "(1) offences against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related offences (computer-related fraud and forgery); (3) content-related offences (child pornography); and (4) criminal copyright infringement." [61].

Hence, the Convention creates a standard policy for state parties for fighting against cybercrime, by adopting appropriate national legislation as well as promoting international co-operation with due respect to human rights in the information society [62].

3.9.2 AU Convention on Cyber Security and Personal Data Protection

The rapid growth and expansion of ICT infrastructures throughout the continent have led to an increasing number of cybercriminals; report shows that in the year of 2016 Africa lost an estimated amount of 550 million USD from cyber-attack [63], this has triggered African Union to enact the Convention on Cyber Security and Personal Data.

The Convention imposes responsibility on its member states to formulate policy and legal frameworks, including establishment of institutions such as CERT or CSIRT to foster cybersecurity governance and for controlling cybercrime [64]. The Convention address a broad range of issues such as Personal Data Protection, Cyber governance, and Personal Electronic Transactions [17].

However, compared to the European Convention on Cyber Crime the AU Convention on Cyber Security and Personal Data Protection is unnecessarily very broad or vague while trying to address different areas which can be addressed separately, this makes it harder to countries to deal with the limited or vague provisions of the AU Convention [17].

So far other sub-regional conventions have also been enacted to such as:

- Legal Framework for Cyber laws of the East African Community.
- Directive on Fighting Cybercrime of ECOWAS;
- Cyber Security Draft Model of COMESA;
- Model Law on Computer Crime and Cybercrime of SADC.

One of the main difference of the two conventions is that the European Convention on Cyber Crime promotes effective and functional ways for international cooperation whereas the Malabo Convention(AU Convention on Cyber Security and Personal Data Protection) does not provide such provision [65].

3.10 Existing Frameworks and Practical Guidelines

In this section, we will analyze some of the selected national cybersecurity strategy development frameworks and guidelines.

3.10.1 ITU National Cyber Security Strategy Guide

ITU is a specialized information and communication agency of the United Nations which responsible for developing technical standards and enhance confidence and security on access to ICT worldwide [62].

On 2011 ITU introduced member states with a reference guide for developing an effective National cybersecurity strategy, this guide can be used by countries to gain knowledge on the purpose and content of the NCSS [61]. This guide focuses on policymakers, public and private stakeholders and issues to be considered by the countries on NCSS development. The guideline addresses different phases of the development life cycle as Initiation; Stocktaking and Analysis; Production; Implementation; Monitoring and evaluation phases [62].

This guideline is prescribed for adoption by all interested countries and prompts a multi-stakeholders approach as well as it supports continuous monitoring and periodic review on the strategy development [62].

3.10.2 ENISA Guidebook on NCSS

With the ever-changing cyber threat environment, ENISA collaborates with different member states and private sectors of the European Union for delivering support on policy-making and implementation and advises, which also includes the development of National Cyber Security Strategy good practice guide and data protection issues [24].

On 2012 ENISA published the first National Cyber Security Strategy Good Practice Guide, which analyses NCSS performance across the member states and EFTA area, the updated NCSS good practice guide of 2016 address six steps on designing and implementing NCSS which are:

1. Set the vision, scope, objectives, and priorities; 2. Follow a risk assessment approach; 3. Take stock of existing policies, regulations, and capabilities;	4. Identify and engage stakeholders; 5. Set a clear governance structure; 6. Establish trusted information-sharing mechanisms [24].

Table 2 ENISA steps on designing and implementing NSCS [24].

Besides the following objectives, it also sets fifteen other objectives on the implementation of National Cybersecurity Strategy and key performance indicators.

This guide identifies essential components of NCSS and which can be used as a cyber-security governance tool by EU and non-EU member states to better address and improve cybersecurity resilience in the country [24].

3.10.3 Commonwealth Approach for Developing NCSS

The CTO is a commonwealth intergovernmental organization which works on Social and economic development and usage through ICT, CTO has developed the commonwealth approach for developing a national cybersecurity strategy [66].

This document addresses the criticality of NCSS for a country and is made with four commonwealth cyber governance principles which include safe and an effective global Cyberspace; broader economic and social development; tackle cybercrime individually and collectively; exercise rights and responsibilities in Cyberspace [66]. This framework is made to be adopted by the member states to help on the process of developing national cybersecurity.

3.10.4 Microsoft

With the essence of supporting governments towards achieving a resilient cybersecurity environment, Microsoft prepared and issued recommendations that can be used by policy makers [67]. Microsoft promotes a risk-based and outcome-focused approach on its strategic principle which also realizes the adoption of an approach to criticality with an understanding of failures are different within key assets and across critical sectors. It also promotes privacy and civil liberty as well as the need to integrate international standards at a high level [67].

3.11 Common Essential Elements of NCSS

This section adapts the recommended content of NCSS by comparing the approach used by different NCSS development guidelines; Newmeyer and Kevin [3] has previously used this approach. This approach was chosen because of the similarity of the purpose of the used approach with our study requirement. This enabled us to extract common characteristics found to be essential to be contained in a typical national cybersecurity strategy which we are going to use it later to evaluate the content of the current Information Security Policy of Ethiopia.

The approach is illustrated below in the table below:

Recommendation	ITU	ENISA	CTO	Microsoft
Top-level government support	✓	✓	✓	✓
National Cybersecurity Coordinator	✓	✓	✓	✓
National Focal Point Organization	✓	✓	✓	✓
Legal framework	✓	✓	✓	✓
National Cybersecurity Framework	✓	✓	✓	✓
CSIRT/CERT	✓	✓	✓	✓
Cybersecurity education and awareness program	✓	✓	✓	✓
Public-private Partnership/Cooperation	✓	✓	✓	✓
Multi-stakeholder approach	✓	X	✓	✓
Cybersecurity workforce skills training	✓	✓	✓	✓
International cooperation	✓	✓	✓	✓
Technical guidelines/ security baselines	X	X	X	✓
Risk assessment process	X	X	✓	✓
Identify critical Infrastructure	X	✓	✓	✓
Cyber exercise and contingency plan	X	✓	**X**	✓
Civil liberties protection	X	X	✓	✓

Table 3 Recommended elements of a National Cybersecurity Strategy [3].

Notes: ✓ = described, X = not describe

3.12 Summary

Various motives, approaches, and process leading to the development of a national cybersecurity strategy have been recognized in this study. It has also been identified that countries should implement international best practices and approaches on their national cybersecurity strategy. On the majority of the studied documents and selected countries policy/strategy analysis, we observed that there are a significant difference in the NCSS development process and approaches. The study has identified that various countries develop NCSS based on national values, ambition, and goals.

Firstly the lack of finding a common definition for terms has been identified as one of the challenges which can potentially cause a significant problem in the context of an international agreement, business objectives, and organizational strategy.

There have been various definitions for terms such as cyberspace, information security, and cybersecurity used by different international guidelines and countries on their NCSS and policy. By analyzing definitions used by international guidelines and countries national cybersecurity strategy and policy, we took definitions which can profoundly suit the purpose of the study.

The study analyses various approaches towards developing national cybersecurity strategy at a national level and address that development and implementation of the NCSS should leverage a multi-stakeholder approach which allows different expertise and various stakeholders in the NCSS development process.

By analyzing various countries cybersecurity policy and strategy, we identified challenges that are faced by other countries in NCSS development process, methods that can be similarly used, and common essential components of NCSS. The collaborative approach between, provincial, territorial, and critical sectors as well as a strong leadership can be taken as best practice from the Canadian NCSS.

Concerning addressing cybersecurity threat Germanys approach to address cybersecurity threats which results from the mismatch between growth in functional development of ICT and country level of cybersecurity readiness which is essential to consider but usually overlooked by other countries.

With a similar, enough previous problem and realities as that of Ethiopian current economy transition and need for a contemporary NCSS, measures that are taken by Singapore on the NCSS development process is taken as a good input to this study.

The Singapore approach to ensure cybersecurity in the form of legislation enacted at the national level, and regulations implemented at the sectoral level, as well as promoting the National Action plan is taken as an input. Rwandan National Cyber Security Strategic Plan was identified to be considered in our study with its nature of providing implementation guidance with a broader context.

The study showed that enacting legislation which is in line with international and regional conventions on cybercrime helps a country to have comprehensive legislation to address the issue of cybercrime. The European Convention on Cybercrime is identified to be the most comprehensive legislation at the international level.

Owning the fact that the European Convention on Cybercrime is the most comprehensive international treaty to address the issue of cybercrime, it laid down the minimum ground which can be followed by nations on legislating cybercrime.

The Ethiopian government has to consider the European Convention on Cyber Crime which can set a baseline and recommend directions to governments, policymakers, law enforcement agencies, and researchers to fight against cybercrime other regional and sub-regional have to be also considered. The study extracted 11 essential elements that satisfy the 60% minimum occurrence criteria content of NCSS and harmonized to evaluate the content of the 2011 Ethiopian National Information Security Policy, and take best practices and approach.

The extracted common essential elements of NCSS are Top-level government support; National Cybersecurity Coordinator; Legal framework; National Cybersecurity Framework; CSIRT/CERT; Cybersecurity education and awareness program; Public-private Partnership/Cooperation; Cybersecurity workforce skills training; International cooperation; Identify critical Infrastructure.

4 Result

In this section, the result of the online questionnaire as well as the interview is presented. The online questioner has been sent to 20 private and public institutions in Ethiopia, and 30 responses were received, 6 out of 30 responses were from private sectors, and the remaining 24 were from government sectors in Ethiopia. The online questionnaire was filled by cybersecurity experts and information technology professionals in the institutions.

4.1 Survey

The online analysis of the survey enabled us to get the current reality of cybercrime in Ethiopia at the institutional level and provided us an understanding of how institutions are responding to cybercrime. The survey covers security agencies, banks, communication, media, and technology service providers.

4.1.1 Survey Analysis

The online survey was conducted anonymously and contained 20 questions; the original instrument can be found in Appendix 1; we categorized the responses into five parts:

1. Respondent work profile and level of reliance on ICT;
2. The current organizational reality, the existence of cybercrime and forms of attacks;
3. A possible source of the cyber-attack and organizational preparation to deal with cyber incidents;
4. Effectiveness of the legal framework in the country regarding cybersecurity.
5. An overall cybersecurity environment in Ethiopia and recommendations.

On our analysis, the first part covered the respondents work profile; hence 30% of the responses were collected from private organizations, and 80% were collected from public organizations:

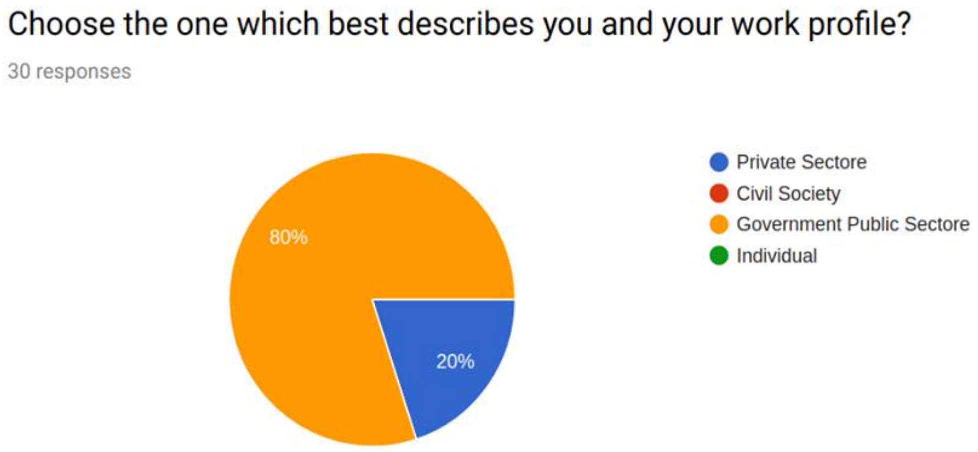


Figure 2 Participant of the survey

This result was due to the state-led development ideology followed by the government of Ethiopia in which the government controls most of the critical sectors.

The other thing to consider was the organization level of reliance on ICT, and from the respondents of the survey, 60% of the organizations were highly reliant on ICT, whereas 33% have medium reliance and the remaining 7% have low reliance.

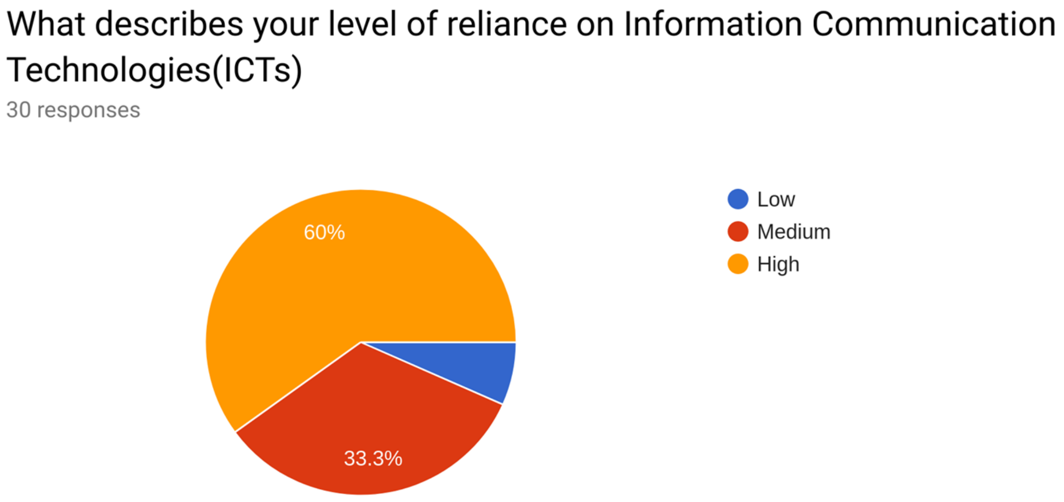


Figure 3 Participant level of reliance on ICT

Considering the fact that a high number of the participant are highly reliant on ICT, from the survey result it is was found that 53.3% of the respondent has encountered a cybercrime incident, and the remaining 30% respondents confirmed that their institution had no cybersecurity incident so far while 16.7% of the respondents are not aware of their organization cybersecurity breach experience.

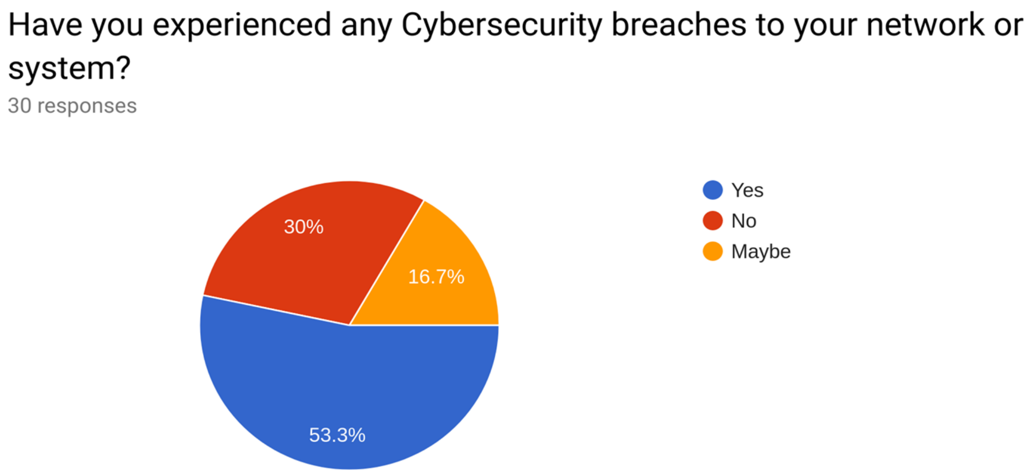


Figure 4 Participant experience of a cybersecurity breach

Depending on the cyber incident experienced by the organizations 19 of the 30 respondents answered the question and it was also found that seven forms of attacks were experienced so far, out of the seven forms of attack the respondents have encountered 89.5% of worms, virus, malware, and another malicious attack, 10.5% website defacement, 15.8% password based attacks, 26.3% phishing attacks, 15.8% session hijacking and Man in the middle attack, 10.5% Cross-site scripting attack, and 10.5% Denial of Service attack.

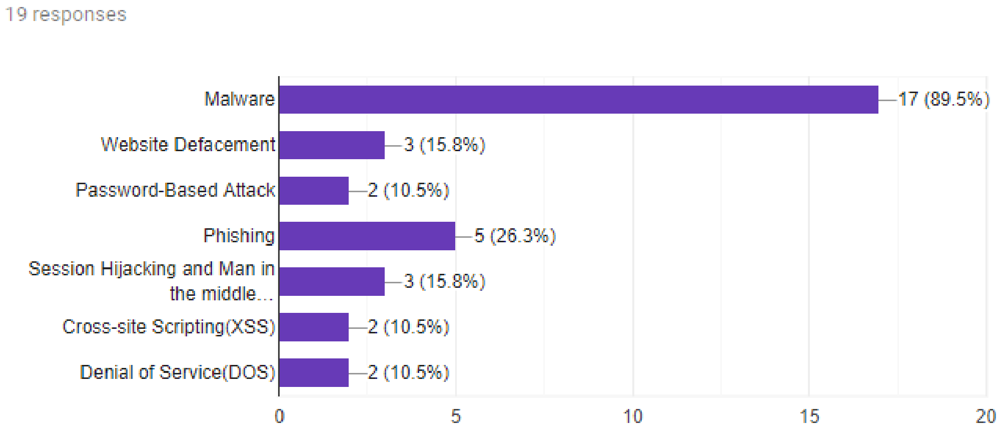
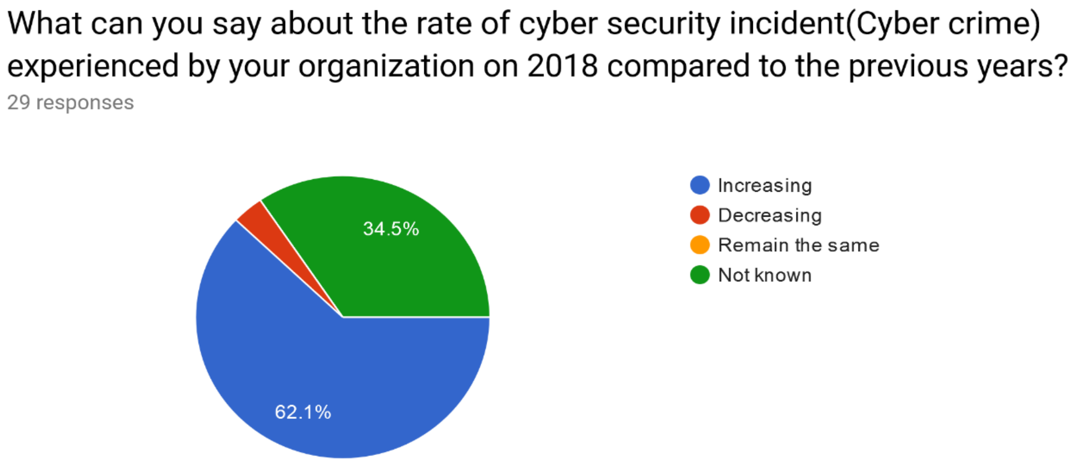


Figure 5 Cybersecurity incident committed against the organization

From the response, we can understand that a large number of cyber incidents happened because of Malware and phishing.

The majority of the respondents 62.1% has also indicated that cybercrime is increasing in their institution compared to the previous years while 34.5% do not know the status, whereas 3.4% of the respondent indicated that cybersecurity incident in their institution is decreasing.

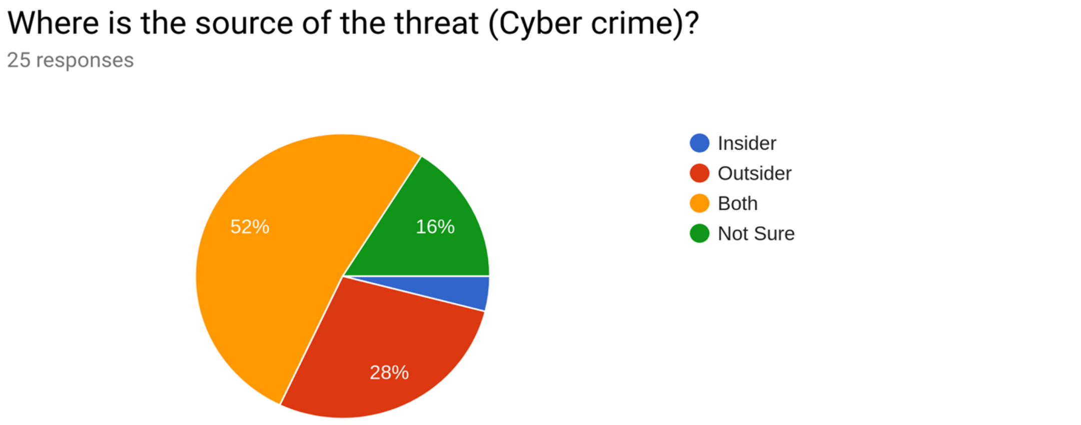


What can you say about the rate of cyber security incident(Cyber crime) experienced by your organization on 2018 compared to the previous years?

29 responses

Figure 6 Rate of a cybersecurity incident in organizations

The respondents indicated the possible source of the cyber-attack. Hence 52% of them were found to be from both outside and inside, whereas 4% are from insider and 28% are shown to be from outsiders while the remaining 16% of the respondents are not sure of the source.



Where is the source of the threat (Cyber crime)?

25 responses

Figure 7 Source of cyber threat in the organization

The survey was also used to examine the level of reporting cyber incidents to the law enforcement a large number of the respondents 78.9% said that is not effective and there are no adequate mechanisms that are placed in the national level.

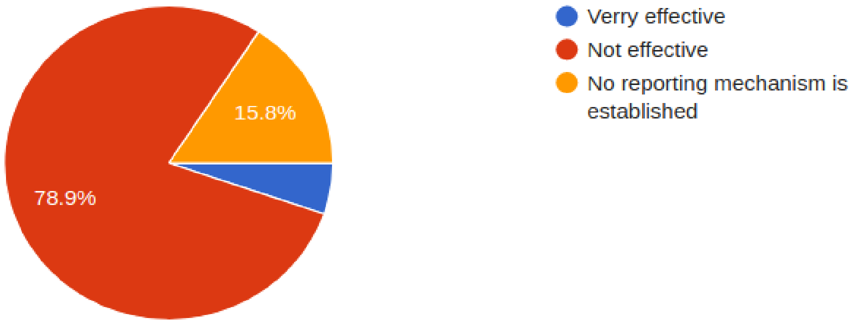
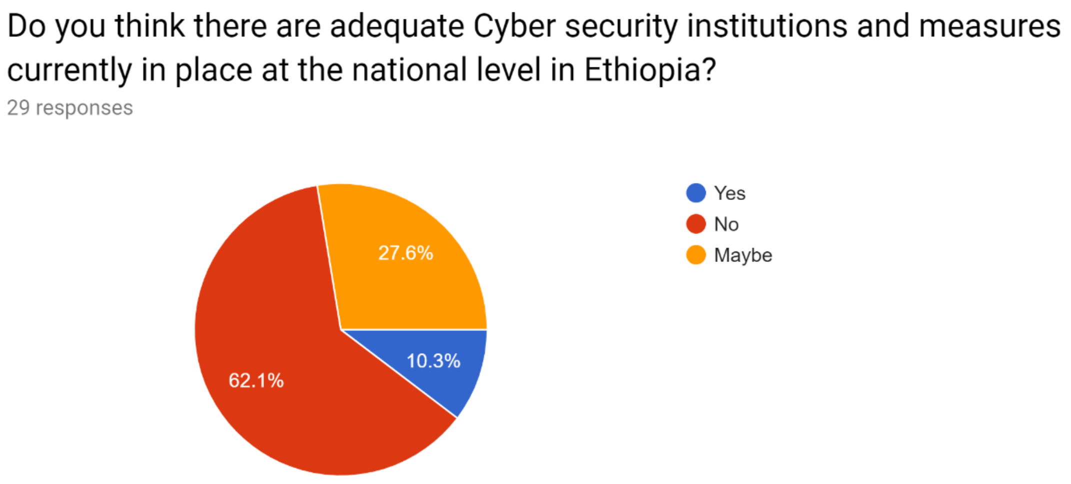


Figure 8 Cybercrime incident reporting mechanism

Regarding the legal framework and regulatory institutions, 29 of the 30 respondents answered the question and 62.1% of the respondent indicated that there is no adequate legal frameworks and measures placed at national level in Ethiopia, whereas 10.3% of the respondent believes that there are adequate measure in place, the remaining(37.6% are not sure whether there are adequate measure is in place.


Do you think there are adequate Cyber security institutions and measures currently in place at the national level in Ethiopia?

29 responses

Figure 9 Cybersecurity institutions and measures in place

Majority of the respondents has also commented that the country is not prepared for cyber-attacks both at an organizational level (policies) and technical capabilities of handling incidents (technical skills).

While others appreciate the contemporary government initiatives concerning adopting cyber Security policies and building the concerned institutions whereas point out that there is a lack of awareness and attention on cyber-security, and all the respondents agreed on strict policy needs to be designed and implemented, The respondent observation on the overall cybersecurity environment of Ethiopia can be found in Appendix 2.

4.2 Interviews

For this study, semi-structured interview was also conducted. Before conducting the interview, we studied existing data and literature carefully to gain an insight into the concept of NCSS design and development. For this study five experts in the area of national cybersecurity strategy development, and policy-making were interviewed, three of them were foreign experts from Estonia, Germany, Nigeria whereas the other two were from Ethiopia.

In order to protect interviewees confidentiality ,the original name of the interviewees was kept private, and an alias was used. Different channels were used to conduct the interview; four of the interviews were conducted through electronic medium Skype, whereas one is conducted face to face.

The interview started with an invitation of the respondents via email with an explanation of the theme and intent of the research, then after, possible time was scheduled, and the interview lasted from 30 minutes to one hour. The interview was recorded and saved and transcribed into text format; the original instrument of the interview can be found in Appendix 3. After the interviews are transcribed, they were ready to be analyzed.

4.2.1 Interview Analysis

The transcribed interview data were analyzed thematically and grouped under five main categories based on the key terms and concepts; the transcribed data was put with anonymous names.

- Purpose of National Cybersecurity Strategy
- Motives of NCSS Development
- Best Practices and International guidelines
- Stakeholder Involvement
- Challenges on NCSS development

Purpose of NCSS

To identify the purpose of NCSS for a country, the interviewees were asked to describe the purpose of NCSS. The overview of the answers from the respondent is presented in the following table:

Alias	Responses
Brad	"The NCSS is used to provide clear guidance and instruction and determine the size, scope, and scale of what the strategy meant to do. NCSS has to be as inclusive as possible."
Chris	"NCSS make sure the state move in an organized manner in the same direction." "Used to coordinate goals efforts will and it mainly depends on the goal of the strategy."
Maya	"NCSS aimed to give a national response to cyber threats."
Robert	"NCSS helps in securing the digital environment of a country."

Kayla	“The NCSS can be used as a roadmap to secure the national infrastructure and services.”

Table 4 Purpose of NCSS

On looking at the purpose of NCSS, the answer from the interview resulted in NCSS to be understood to provide clear guidance, and instruction to secure the national digital environment from cyber threat as well as make sure the country move in an organized manner.

Motives towards NCSS Development

Given various motives towards national cybersecurity strategy development the interviewees describe motives in NCSS development as follow:

Alias	Responses
Brad	“Protect national sovereignty; make business better; promote education ”
Chris	“The strategy depends on the goal, to improve the situation or to maintain what exists ”
Maya	“To ensure cybersecurity in the countries digital environment ”
Robert	“To give a national response to a cybersecurity threat and strengthen national resilience.”
Kayla	“To promote international cooperation and reduce the national cybersecurity threat ”

Table 5 Motives towards NCSS development

The interview result clearly shows that there are different motives that lead countries to the development of NCSS which includes the protection on national sovereignty; economy reasons; improving cybersecurity situations in the country; ensuring cybersecurity in the digital environment; to respond to a cyber threat; promote international cooperation and reduce cyber threats.

Best Practices and International Guidelines

To understand how countries should take best practices and international guidance on developing NCSS, the interviewees were asked how the best practices, international guidelines, models, and templates can be used in the NCSS development process.

Alias	Responses
Brad	“Each country has to decide this out on the applicability of the international standard, law, state behavior in the cyberspace, and what are non-binding norms ” “International guidelines and best practice can be used as a baseline on designing national cybersecurity strategy.” “Countries should have their guideline; there is no one right size framework which feet’s every country and should look its political context.”
Chris	“Counties can take the best practice of other countries and learn from previous iterations, adapt frameworks to countries circumstance.”
Maya	“Countries can adapt strategies international guidance and tailor it to their context ” “Each country should have its guidelines tailored to their peculiarities and environment.”
Robert	“Cybersecurity is not limited to a very specific country. When developing national cybersecurity policy,

	benchmarking is essential for the quality of the national cybersecurity policy. This does not mean we don’t have to consider our national context.”
Kayla	“Countries can follow best practices and international standards which are provided by different organizations such as ITU on their NCSS development process.”

Table 6 Best practices and international guidelines

The result collected from the interview shows that international guidance, models, and best practices can be used as a baseline in NCSS development process, and these guidelines and best practices should be tailored to fit the national context.

Stakeholder Involvement

To identify and understand who should participate in the national cybersecurity strategy development process the interview asked respondents to specify who should participate in NCSS development.

Alias	Responses
Brad	“There need to be an open dialogue with the whole society and the private sectors and provide an opportunity for them to contribute to the national strategy ”
Chris	“Document is for the government and so that it is mainly government dominated, but private included, the goal is private sectors should collaborate.”
Maya	“Strategies cannot be built from just public perspective; it should also consider the private sectors because most infrastructures are owned by the private sector.”

Robert	“Cybersecurity stakeholders which include government organizations, private sectors, Academia, and civil society organizations.”
Kayla	“The public, as well as the private sectors, should participate as a task force on the development as well as a review of the document process.”

Table 7 Stakeholder involvement

As we can observe from the interview result, when developing NCSS it is necessary to include all stakeholders, including the public sectors and private sector as well as civil society.

Challenges in NCSS Development

By considering various challenges on design and development of NCSS the interviewees describe major challenges as follow:

Alias	Responses
Brad	“Bringing Cyber Security theme to a high level of priority where serving political leaders and citizens.”
Maya	“The challenges on developing national cybersecurity strategy lack of resource as well as complimentary plan to implement.”
Robert	“Resource, capital, talent and getting a political mandate from the government or legislator.”
Kayla	“Addressing the applicability of international law, and state behavior on cyberspace as well as non-binding norms.”

Table 8 Challenges in NCSS development

As we can observe from the result of the interview, national cybersecurity strategy is essential for countries to create secure and resilient cyberspace by providing clear guidance and instruction as well as allowing states to move forward in an organized manner.

Countries can adapt international guidance to their own circumstance and take the best practice of other countries as well as learn from previous iterations. Bringing cybersecurity theme to a high level of priority, lack of resource, capital, talent, and complementary action plan, as well as challenges on addressing the applicability of international law, and state behavior on cyberspace are identified from the interview as major challenges.

5 Findings and Discussion

National Cybersecurity Strategy is a useful tool to solve cybersecurity problems at a national level, and its development needs a high effort from government and all stakeholders. The Ethiopian government should recognize the growth of cyber threat in the country and take adequate strategic measures to address it

These measures include developing and implementing a comprehensive national cybersecurity strategy which is tailored to the country strategic objectives, goals, and priorities. The 2011 National Information Security Policy is the closest strategic document which addresses cybersecurity at a national level. However, it fails to address the country current cybersecurity environment and also does not provide conditions to adequately address the notion of critical infrastructure, links with other national and international strategies, public-private partnership, and update or review mechanism.

International guidelines and frameworks can be used as a baseline to develop NCSS; however, which guiding principles to follow and how to implement are different across countries. The transfer of these guidelines as it is, to a developing country like Ethiopia is not acceptable, and it could create problems on future operations as well as cybersecurity response level.

In this section, we evaluate the content of the 2011 National Information Security Policy of Ethiopia based on the harmonized essential elements of NCSS, and we will propose guidelines for a new National Cybersecurity Strategy which is tailored with the national ambition, resource, and priority areas.

5.1 Content Evaluation of Ethiopian NISP of 2011

To identify gaps and shortcomings of the National Information Security Policy of 2011, we evaluated the policy based on the 60 percent minimum content occurrence criterion, within the examined recommended elements of NCSS in the previous chapter, the identified elements which full fills the criteria are taken as essential elements that any comprehensive NCSS should address. This approach has been previously used by the study in [46], and it is taken because of its resemblance to our context of the study.

From Table 3 Recommended elements of a National Cybersecurity Strategy. We were able to identify 11 common essential elements that satisfy the 60% minimum occurrence criteria these are: Top-level government support; National Cybersecurity Coordinator; Legal framework; National Cybersecurity Framework; CSIRT/CERT; Cybersecurity education and awareness program; Public-private Partnership/Cooperation; Cybersecurity workforce skills training; International cooperation; Identify critical Infrastructure.

1. Top-level government support: It is reflected in the information security policy that the government has to take the leadership role and give support on policy implementation [10].
2. National Cybersecurity Coordinator: The policy address the necessity of establishing a cybersecurity coordinator institution, and state that Ethiopian Information Network Security Agency (INSA) as one institutional building block [10].
3. Legal framework: The policy made provision to promote legal framework, formulation of laws, and the adoption of regulatory procedures. It is stated in the policy that the government is going to be responsible and committed for appropriate legal measures and strategy implementation [10].
4. National Cybersecurity Framework: The policy fails to address the adoption of a framework which enables countries to define the minimum security requirement.
5. CSIRT/CERT: The policy address the need for organizations which acts as a point of contact to the establishment of CERT.
6. Cybersecurity education and awareness program: The policy prompts information security training and education and builds national capability by increasing the number of information security professionals.
7. Public-private Partnership/Cooperation: The policy fails to address public, private partnership.
8. Cybersecurity workforce skills training: The policy address the need for training and educational programs to promote useful security knowledge and skills within the workforce [10].
9. International cooperation: The policy implies the need for international cooperation but fails to address it sufficiently.

10. Identify critical Infrastructure: It is barely implied in the policy and needs to be clearly addressed.

By assessing individual criteria separately, the output of the study shows that there are different conformity figures with the chosen criterion. Even though the current effective information security policy constitutes quite a significant step forward, the finding of the comparative study shows the fact that the policy has the following significant shortcomings it lacks certain aspects and contents which appear to be critical to Ethiopian environment such as:

- Fails to identify scope/areas of critical infrastructure and industries;
- Fails to promote National Cybersecurity Framework;
- Fails to address International cooperation adequately;
- Lack of including public and private partnership;
- Lack to specify a review mechanism;
- Fails to specify an action plan;
- Lack of explaining the current national cybersecurity state;

Besides the policy mentioned above INSA has enacted Critical Mass Cyber Security Requirement Standard document in 2018 as an implementation plan, which enforces organizations to build cybersecurity capability and establish adequate security measures to manage internal security risks [68].

Based on our survey and content analyses, the major significant challenges, gaps, and weakness of the national cybersecurity environment are synthesized and described as follows:

- An inadequate legal framework to support cybersecurity;
- Poor IT security infrastructure;
- Lack of Cyber Security awareness and culture;
- Poor public and private sectors cooperation;
- Lack of research and development;
- Lack of coordination within the Federal and regional government;
- Lack of international cooperation;
- Inadequate skills, resource, and capacity.

Hence, in this research, the proposed guidelines should consistently focus on the principles that better address the significant challenges in the country such as:

- Effective governance and Establishment of an institutional framework.
- Identify and define resources, methods, approaches of critical infrastructure.
- Active cybersecurity culture and capacity building.
- Cooperation within the Federal and regional government.
- Cooperation within the public and private sectors.
- Collaboration and cooperation with international experts and organizations.
- Competent legal and regulatory framework.

5.2 Proposed Guidelines for Future Ethiopian NCSS

By assessing the experiences of other countries cybersecurity strategy and various international guidelines, by examining the national view of the cyberspace and contemporary cybersecurity challenges, legal measures in place in Ethiopia, by synthesizing the knowledge from subject matter experts from the semi-structured interview as well as based on the existing institutional framework.

We recommend and specify guidelines for future comprehensive NCSS Strategy in Ethiopia which meets the countries contemporary national strategic objectives, goals, and priorities as follows:

5.2.1 Scope and Strategic Direction

The scope of the NCSS should include all actors at governmental, national, and international level, all processed or not processed information, all medium used, all physical and information infrastructure where information is collected, transmitted, stored and processed.

The scope of the national cybersecurity should also consider needs which are difficult to choose such as, promote economic growth with usage of new technology and the increase in security risk; data protection and information sharing; freedom of speech and political stability; public and private sector regulatory approaches, infrastructure modernization and critical infrastructure protection [7] [9].

Strategic directions can be derived for the countries long term plan and vision. The national vision is described in the 2011 National Information Security Policy of Ethiopia as “To transform Ethiopia from a poverty-stricken country to a middle-income economy and society with deep-rooted participatory democracy and good governance based on the mutual aspiration of its peoples” [10].

Ethiopian growth and transformation plan (GTP II) is also one of the central planning document of the country; the strategic directions for digital infrastructure are stated as:

- To increase the speed of ICT development, to strengthen legal framework and security;
- To integrate ICT into government administration;
- To upgrade infrastructure and services;
- To create awareness of ICT usage among the general public, and strengthen research and development [18].

Other strategic directions stated in the GTPII of Ethiopia address minimizing the use of second-generation mobiles in the country from 93 percent in 2014/15 to 47% by 2019/20, increase engagement of private sectors, broaden internet usage across government offices, and formulate strategies [18].

5.2.2 NCSS relation to other documents

NCSS cannot exist alone; it has to be linked and consistent with other domestic guidelines, policies, and development plans, which mainly deal with ICT and critical information systems dependent sectors [9]. The NCSS diverges from existing policies and mostly be linked with the countries national security strategy and national ICT policy and strategy.

Ethiopian foreign and national security policy address that national interest and security can be achieved through economic development, and identify internal threats which may result from an absence of democracy, lack of good governance, and poverty as the main security threat of the country [69]. From this, we can understand that Ethiopian national security is tailored with internal economic development.

Cyberspace and security are not identified in the document as another dimension of security threat, though NCSS can be viewed as a complement to the country national security policy in such a way that by strengthening the cybersecurity of national information resources and infrastructures.

The NCSS should also be linked with the national information and communication technology policy and strategy of Ethiopian. The ICTPS focuses on nine key areas: Development of ICT infrastructure; Development Human resource; ICT's legal systems and security; E-Government; ICT in the education sector; ICT for improved health; ICT for agricultural modernization; Development of ICT industry and private sector; ICT for research and development [34].

Hence, to avoid any duplication and conflicting principles between strategies, policies, action plans it is necessary to prepare concrete proposals [9].

5.2.3 Effective Governance

Cyber-attacks are becoming a threat to not only for the single institution but also to national security [2] with this in mind it is the responsibility of any government to safeguard the national security, by having effective governance.

According to [9]"Any approach to NCS strategy needs to consider the 'three dimensions' of activity: the government, the national (or societal) and international.".

With the involvement of different forms of stakeholders such as the civil society, military, law enforcement, judicial, commerce, infrastructure, private institutions, intelligence and other government institutions that are claiming responsibly for national cybersecurity, triggers the need to have effective coordination between them [9].

As we observed from our study the measures that are taken by the government of Ethiopia in addressing cybersecurity is law paced, hence the future NCSS of Ethiopia should prompt the federal government of Ethiopia to play the leadership role in the implementation of the national cybersecurity strategy and action plan. Which can be achieved through increased horizontal collaboration and accountability among government sectors as well as private sectors, civil society, regions, and international institutions.

Due to the borderless nature of cyber threat, the NCSS should consider cooperation at regional and international level, international cooperation is linked to the country's foreign policy; the county needs a more proactive rather than reactive foreign policy and it should be stated on the NSS describing how the country act in international affairs [9].

The existing Ethiopian foreign policy is based on the inside-out approach in which international agreements and corporations are made based on the mutual interest and equality of the states with priorities to the national interest and security [69].

The national cybersecurity strategy will become useless without the crucial support of political leaders, political will is essential for the practical implementation of a strategy [3], in the case of Ethiopia with a parliamentary nature of the government, this political will or guidance can be found from the prime minister of the country.

Which can be achieved through:

- Establish a dedicated institution which regulates, and handle cybersecurity issues at the federal level;
- Promote a centralized planning and decentralized execution across federal and regional sectors.
- Establishing an effective NCS organizational framework;
- Reinforcing the analysis and response capability of government ministries;
- Establish incident reporting mechanisms;
- Promote international cooperation;

5.2.4 Legal Controls

As we can see and understand from our study the current effective legal framework in the country is not adequately addressing cybercrime situation in the country. The future NCSS of Ethiopia has to identify and implement a suitable and adequate legal framework which helps to address and prosecute cybercrime.

According to NCSFM, “A national cybersecurity strategy should not exist in a strategic vacuum.” [7]. It should be developed in such a way that it is linked with existing international and regional conventions, directives, and with domestic legislation, guidelines this promotes coordination, cooperation, and collaboration [7].

The cybersecurity of critical infrastructures can be assured through the development of a legal framework which will also establish common security standards which can be applied for all actors involved in the usage of ICT.

By understanding the gaps and challenges within the contemporary legal framework in Ethiopia, the cybercrime legislation should consider the following international and domestic legislation:

- European Convention on Cyber Crime [58];
- AU Convention on Cybersecurity and Personal data protection[56];
- National Payment System Proclamation [30];
- Registration of Vital Events and National Identity Card Proclamation [31];
- Telecom Fraud Proclamation [32];
- Computer Crime Proclamation [70];

The goal for the development of a legal framework can be stated as follow:

- Establish a minimum security requirement standard for all information systems.
- Enforce the existing critical mass cybersecurity requirement standard.
- Develop a unified cybersecurity and cybercrime definition in the entire legal regulations.
- Enhance the existing legislation.
- Examine the usage and necessity of legal acts.
- Draft new legislation for covering new areas of cyber threat.
- Promote international and regional cooperation.

Also, the Ethiopian National Cyber Security Strategy should guarantee the normal functioning of a legal framework in the area of cybersecurity, promote amendments on legal acts and establish law enforcement units.

5.2.5 Cybersecurity Culture and Capacity Building

Our study identified that there is a low cybersecurity culture in the country and promoting cybersecurity culture and engaging in capacity building programs have enormous benefit to ensure a secure cyber environment. Capacity building is defined in this study as the steps that are taken towards growing the skills, knowledge, and competency level of individuals, communities, and government [71].

Countries have different priority areas in capacity building [72] with the shortage of skilled cybersecurity professionals and low competency level of cybersecurity professionals across public and private sectors in Ethiopia. The future NCSS of Ethiopia should prompt cybersecurity capacity building programs, through knowledge building, skill sharing, technical and equipment support. Hence this can be achieved through:

- Promote capacity building through international collaboration and partnership with like-minded partners.
- Ensuring cybersecurity literacy and awareness in government, the private sector and civil society.
- Promote strategic and organizational basis to establish coordination among public and private sectors through information sharing.
- Develop essential skills and R&D capability.
- Develop a cybersecurity index measure to identify the maturity level of cybersecurity culture across government and private sectors.
- Promote education on cybersecurity for schools and universities.
- Promote a national cybersecurity awareness campaign.

5.2.6 Critical Infrastructure and Assets

Critical infrastructures are defined in this study as private, or government institution or organizations which give essential service for the public good, whose damage may result in immense security or other harm on the society [9].

According to [9] critical infrastructure and industries have become the primary target of most recent cyber-attacks. As we can observe from our study, there are no adequate measures placed in Ethiopia to protect the information and physical critical infrastructures from any form of cyber threat

So the scope and area of critical infrastructure should be defined in the future NCSS of Ethiopia, in such a way that it includes both the information as well as physical infrastructure that helps for ensuring the secure delivery of essential services, and should identify critical sectors or institutions this may include:

- Health service institutions: Hospitals, Laboratories.
- Transport Service institution: Airport, Traffic control system.
- Power grid: Hydropower dam control systems which primarily include The Great Ethiopian Renaissance Dam.
- Finance and insurance: Bank and Financial Institutions.
- ICT: Telecommunication, Internet infrastructure, Internet Service provider, Service payment centers.
- Media: The National Broadcast Cooperation.

Thus this can be achieved through:

- Identifying resources which support critical functions.
- Defining Methods or Approaches to critical infrastructure.
- Promoting and identifying response mechanism for a cybersecurity incident.
- Promoting and identifying recovery mechanisms from a cybersecurity incident.

5.2.7 Stakeholder Engagement

According to ITU NCSS Guide, collaboration among government, the private sector, and civil society are very crucial in the development of national cybersecurity strategy [62].

The NCSS should enable the government to take the lead on coordinating the cooperation and ensuring that all stakeholders are part of the strategic development throughout the implementation and this can be achieved through:

- Establish a public-private partnership.
- Strengthening and maintaining cooperation within the Federal government and among the public and private sectors.
- Develop national stakeholder monitoring and engagement plan.
- Promote small cybersecurity business.
- Establishing international partnerships.

5.2.8 Technical and procedural measures

We can observe from our study that major cyber threats in Ethiopia are caused by Malware and phishing, by considering these and the overall cyber threat environment in public and private organizations in Ethiopia as well as by understanding the non-static nature of the cyber threat.

The future NCSS of Ethiopia should address security control and measures that are needed to assure the country cybersecurity readiness in mitigating risk and protecting the confidentiality, integrity, and availability of critical information assets.

And this can be achieved through the following considerations and technological measures:

- Take best practice from countries with high cybersecurity profiles;
- Enforce the implementation of the existing critical mass cybersecurity requirement standards.
- Take consideration of international standards such as(ISO 27001/27002, CIS critical security control, NIST framework)
- Promote research and development by integrating cybersecurity in the educational curriculum.

6 Conclusion

The aim of the study was to propose guidelines for the Ethiopia National Cybersecurity Strategy. To achieve the purpose we studied the cybersecurity environment in Ethiopia based on domestic guidelines and questionnaire administered online; analysis of different approaches, countries best practices and international guidelines; analysis of data collected with the interview from various subject matter experts.

Designing NCSS requires the understanding of the national context in the area of cybersecurity which can be determined by various measures. The national context of cybersecurity in Ethiopia can be presented concerning the usage of ICT infrastructure and ICT-based services.

The result of the study shows that the contemporary state of cybersecurity in Ethiopia lack effective measures to fight against cyber incidents, which have resulted in the growth of cybercrime in the country.

The Ethiopian government is working towards fighting against the cyber threat by putting in place different policies and legislation. However, this effort is not enough and much work needed to address the evolving and constantly changing nature of the cyber threat.

The shift in the Ethiopian economy policy from strong government involvement in various key sectors to deregulation and privatization of critical infrastructures urges the need to develop a more consistent NCSS which involves the cooperation of public and private sectors in the strategic planning and process.

Based on the study conducted, the existing cybersecurity regulatory institutions, policies, and legislation in Ethiopia can be enhanced to correspond with international standards and principles through the development of a more consistent NCSS.

The result of the study can be used by the national government and policy makers in Ethiopia to develop a more consistent national cybersecurity strategy which is tailored with the national ambition, resource, goals, and priority.

Additionally, with the absence of similar research which addresses the development of a national cybersecurity strategy in Ethiopia, this research can be used as a knowledge base for future research on the area. This study proposes guidelines to develop NCSS in Ethiopia, in future research the proposed guidelines can be tested in a real situation, as well as the theme of the national cybersecurity action plan does not address on the study and left for future researchers on the area.

7 Bibliography

[1] E. L. C. M. D. a. Z. M. Schomakers, " Internet users’ perceptions of information sensitivity – insights from Germany.," *International Journal of Information Management*, pp. 46,142-150, 2017.

[2] C. O. R. a. T. A. Czosseck, "Estonia after the 2007 Cyber Attacks," *International Journal of Cyber Warfare and Terrorism,* vol. 1, no. 1, pp. 22-34, 2011.

[3] K. P.Newmeyer, "Elements of National Cybersecurity Strategy for Developing Nations," *National Cybersecurity Institute Journal,* vol. 1, no. 3, pp. 11,48,16,10, 2015.

[4] C. J. S. Schjølberg, "ITU Global Cybersecurity Agenda High-Level Experts Group,"Judge at the Moss Tingrett Court, Norway, 2008.

[5] M. Kerttunen, "National Cyber Security Strategies :A Commitment to Development,"APNIC, 4 April 2019. [Online]. Available: https://blog.apnic.net/2019/04/04/national-cybersecurity-strategies-commitment-to-development/. [Accessed 14 April 2019].

[6] T. V. V. RUDN, "The Role of Cybersecurity in World Politics," *International Relations,* vol. 17, no. 2, pp. 339-348, 2017.

[7] (Ed.), Alexander Klimburg, "National Cyber Security Framework Manual," NATO CCD COE Publication, Tallinn, 2012.

[8] ITU, " ITU National Cybersecurity Strategy Guide," ITU, Geneva, 2011. [Online]. Available: http://www.itu.int/ITUD/cyb/cybersecurity/docs/ ITUNationalCybersecurityStrategyGuide.pdf . [Accessed 14 April 2019]

[9] K. K. Anna-Maria Osula, "NATO CCD COE National Cyber Security Strategy Guidelines," NATO CCD COE, Tallinn, 2013. . [Online]. Available: https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf . [Accessed 15 January 2018]

[10] The Federal Democratic Republic of Ethiopia,, "National Information Security Policy," Information Network Security Agency, 09 2011. [Online]. Available: http://www.insa.gov.et/documents/10184/13629/National+Informattion+Security +Policy.pdf/9dfc9c1d-19b9-4b78-9d15-ede5310fd6cf. [Accessed 6 11 2018].

[11] Aaron Maasho, "REUTERS," 6 June 2018. [Online]. Available: https://www.reuters.com/article/us-ethiopia-privatisation/ethiopia-loosens -throttle-on-many-key-sectors-but-privatization-still-far-off-idUSKCN1J21QV. [Accessed 5 January 2019].

[12] "National Cyber Security Index," [Online]. Available: https://ncsi.ega.ee/. [Accessed 15 January 2018].

[13] K. S.-F. K. B. Naomi Oreskes, "Verification, Validation, and Confirmation of Numerical Models in the Earth Sciences," vol. 263, no. 5147, pp. 641-646, 1994.

[14] ENISA, "National Cyber Security Strategies Evaluation Tool," European Union Agency for Network and Information Security.[Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.[Accessed 15 January 2018].

[15] H. Hailu, "Abyssinialaw," [Online]. Available: https://www.abyssinialaw.com/blog-posts/item/1545-the-state-of-cybercrime-governance-in-ethiopia. [Accessed 15 January 2018].

[16] S. KEMP, "Digital in 2018," Hootsuite, 2018. [Online]. Available: https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338 [Accessed 2019 03 12].

[17] I. Teketel, "Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences," 01 2018. [Online]. Available: http://etd.aau.edu.et/bitstream/handle/123456789/12648/Iyasu%20Teketel.pdf?sequence=1&isAllowed=y. [Accessed 2019 03 12].

[18] National Planning Commission, "Growth and Transformation Plan II (GTP II) (2015/16-2019/20)," National Planning Commission, 2016. [Online]. Available: https://europa.eu/capacity4dev/resilience_ethiopia/document/growth-andtransformation-plan-ii-gtp-ii-201516-201920 . [Accessed 2019 03 12].

[19] A. Arman, "Foreign Policy Association," 28 March 2018. [Online]. Available: https://foreignpolicyblogs.com/2018/03/28/regional-and-geopolitical-impact-of-ethiopia-meltdown/. [Accessed 2 February 2019].

[20] Ezega, "Ezega News," 2017. [Online]. Available: https://www.ezega.com/News/NewsDetails/4202/INSA-Reports-Ethiopia-Hit-by-256-Cyber-Attacks-in-Six-Months.[Accessed 25 February 2019].

[21] UN News, "UN News," 22 September 2016. [Online]. Available: https://news.un.org/en/story/2016/09/540022-ethiopian-leader-un-assembly-decries-use-social-media-spread-messages-hate-and. [Accessed 2 February 2019].

[22] G. A. S. M. J. S.-R. a. R. D. Bill Marczak, "The Citizen Lab," 6 12 2017. [Online]. Available: https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/. [Accessed 25 February 2019].

[23] Kaspersky lab, "Kaspersky Security Bulletin," 2017. [Online]. Available: https://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2017_Statistics-PR-1045.pdf.[Accessed 12 February 2019].

[24] ENISA, "ENISA NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies," ENISA, 2016.

[25] Ministry of Science and Technology, "Ministry of Science and Technology," [Online]. Available: http://www.most.gov.et/about-us . [Accessed 3 March 2019].

[26] Ministry of Innovation and Technology, "MCIT," [Online]. Available: http://www.mcit.gov.et/web/guest/mandate-and-responsibility. [Accessed 12 March 2019].

[27] The Federal Negarit Gazzete, "Information Network Security Agency Re-stablishment Proclamation," The Federal Democratic Republic of Ethiopia, Addis Ababa, 2014.

[28] The Federal Negarit Gazzeta, "Ethiopian Federal Police Commission Establishment," The Federal Democratic Republic of Ethiopia, Addis Ababa, 2011.

[29] The Federal Negarit Gazette, "National Intelligence and Security Service Re-establishment Proclamation," The Federal Democratic Republic of Ethiopia, Addis Ababa, 2013.

[30] A. YOHANNES, " Chilot," 31 July 2011. [Online]. Available: https://chilot.me/2011/07/proclamation-no-7182011-a-proclamation-to-provide-for-national-payment-system/. [Accessed 18 March 2019].

[31] Federal Democratic Republic of Ethiopia, "Vital Event Registration and National Identity Card proclamation," Federal Democratic Republic of Ethiopia, Addis Ababa, 2017.

[32] The Federal Negarit Gazette, "Proclamation No. 761/2012 Telecom Fraud Offence Proclamation," House of People Representative, Addis Ababa, 2017.

[33] K. M. Yilma, " Some Remarks on Ethiopia's New Cybercrime Legislation," [Online]. Available: https://www.ajol.info/index.php/mlr/article/view/153608. [Accessed 19 March 2019].

[34] Feredal Democratic Republic of Ethiopia, "The National Information and Communication Technology Policy and Strategy," Feredal Democratic Republic of Ethiopia, 2009.

[35] P. R. Y. A, " Development of National Cyber Security Strategies (NCSSs), and an Application of Perspective to the Colombian Case," 2016.

[36] R. K. a. Y. V. K. Audrey, " Critical Terminology Critical Terminology Foundations 2," *EastWest Inst. Inf. Secur. Inst. Moscow State Univ,* vol. 2, 2014.

[37] T. W. Azmi, " Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy," in *Australasian Conference on Information Systems,* Wollongong, 2016.

[38] A. M. Narmeen Student, "Comparative Analysis of Various National Cyber Security Strategies," *International journal of computer science and information security,* vol. 14, no. 1, pp. 131,132, 2016.

[39] R. a. v. N. J. Von Solms, "From information security to cyber security," Computers & Security," *The official journal of Technical Committee 11 (computer security) of the International Federation for Information Processing.,* vol. 38, pp. 97-102, 2013.

[40] D. S. L. K. Matthew Shears, "Multistakeholder Approaches to National Cybersecurity Strategy Development," GLOBAL PARTNERS DIGITAL, 2018.

[41] F. B. S. Deirdre K.Mulligan, "Doctrine for Cybersecurity∗," p. 30, 2011.

[42] E. T. Mika Kerttunen, "Strategically normative. Norms and principles in national cybersecurity strategies," 13 April 2019. [Online]. Available: https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/. [Accessed 15 April 2019].

[43] ITU, "Global Cybersecurity Index.," ITU, 2018. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf. [Accessed 27 11 2018].

[44] "National Cyber Security Strategy: Canada's Vision for Security and," Public Safety Canada, 2018.

[45] V. C. J. C. Regner Sabillon, "National Cyber Security Strategies: Global Trends in Cyberspace," *International Journal of Computer Science and Software Engineering (IJCSSE),* vol. 5, no. 5, p. 68, 2016.

[46] O. Onoja, "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis," *International Journal of Cyber Criminology (IJCC),* vol. 9(1), p. 127, 2015.

[47] "Action Plan for Critical Infrastructure," Public Safety Canada, 2009.

[48] "Cyber Security Strategy for Germany," 2011. [Online]. Available: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile . [Accessed 27 11 2018].

[49] O. Wechsler, "Germany’s Cyber Strategy—Government and Military Preparations for Facing Cyber Threats," *Cyber, Intelligence, and Security |*, vol. 2, no. 1, pp. 1,56, 2018.

[50] K. B. M. S. P. d. G. H.A.M. Luiijf, "Critical Information Infrastructure Security: Ten National Cyber Security Strategies: A Comparison," 2011. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2F978-3-642-41476-3.pdf. [Accessed 11 01 2019].

[51] J. Manalo, "International Association For Political Science Students:03 MARMiracle in marshland: The Singaporean developmental state story," 2015. [Online]. Available: https://iapss.org/2015/03/03/miracle-in-marshland-the-singaporean-developmental-state-story/. [Accessed 5 12 2018].

[52] F. M. Bizuayehu Daba, "Incorporating Democratic Developmental State Ideology into Ethiopia’s Ethnic Federalism – A Contradiction?," *ÜNİVERSİTEPARK Bülten | Bulletin,* vol. 6, no. 1, pp. 109-117, 2017.

[53] "Policy Analysis: Singapore’s Public-Private Partnerships for Cybersecurity in the Critical Infrastructure Sectors — Challenges and Opportunities," Lee Kuan Yew School of Public Policy at the National University of Singapore, 2017, p. 4.

[54] "Singapore’s Cyber security Strategy," Cyber Security Agency of Singapore, 2016.

[55] "Rwanda National Cyber Security Policy," Republic of RwandaMinistry of ICT & Innovation, 2015.

[56] "Rwanda National Cyber Security Strategic Plan," Republic of RwandaMinistry of ICT & Innovation, Kigali, 2015.

[57] "Official Gazette nº 27," 03 7 2017. [Online]. Available: http://minict.gov.rw/fileadmin/Documents/Mitec2018/Policies___Publication/ICT_Laws/Law_establishing_the__NCSA-2-20.pdf . [Accessed 13 03 2019].

[58] Council of Europe, "CONVENTION ON CYBERCRIME," Council of Europe: European Treaty Series - No. 185, Budapest, 2001.

[59] "AU Convention in cybersecurity and personal data protection," The Member States of the African Union, malabo, 2000.

[60] S. S, " Budapest Convention on Cybercrime – An Overview," Center for Communication Governance:, 3 March 2016. [Online]. Available: https://ccgnludelhi.wordpress.com/2016/03/03/budapest-convention-on-cybercrime-an-overview/. [Accessed 19 02 2019].

[61] J. CLOUGH*, "The Budapest Convention on Cybercrime and the Challenges of Harmonisation," in *A World of Difference,* Monash University Law .

[62] ITU, "Guide to Developing National Cybersecurity Strategy," ITU, Geneva, 2018.

[63] "Africa Cyber Security Report," Serianu Cyber Threat Intelligence Team in partnership with the USIU’s Centre for Informatics Research and Innovation (CIRI), 2016.

[64] U. J. Orji, "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?," *Masaryk University Journal of Law and Technology.,* vol. 12, no. 2, p. 91, 2018.

[65] Z. Jamil, "Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime," *Global Action on Cybercrime Extended*, vol. 20, p. 4, 2016.

[66] CTO, "COMMONWEALTH APPROACH FOR DEVELOPING NATIONAL CYBERSECURITY STRATEGIES," CTO, 2015.

[67] J. P. N. Cristin Flynn Goodwin, "Developing a National Strategy," Microsoft , 2013.

[68] Information Network Security Agency, "Critical mass cyber security requirmen," Information Network Security Agency, Addis Ababa, 2018.

[69] Ministry of Information, "The Federal Democratic Republic of Ethiopia Foreign Affairs and National Security Policy and Strategy," Press & Audiovisual Department , Addis Ababa, 2002.

[70] Federal Negarit Gazette, " Computer Crime Proclamation," Hause of People Representative, 2016.

[71] A. P. T. B. Mirko Hohmann, GPPi, 6 March 2017. [Online]. Available: https://www.gppi.net/2017/03/06/advancing-cybersecurity-capacity-building-implementing-a-principle-based-approach. [Accessed 12 March 2019].

[72] P. Pawlak, "Cyber Capacity Building in Tean Points," in *European Union Institute for Security Studies*, Paris, 2014.

[73] L. S. Sterling, The Art of Agent-Oriented Modeling, London: The MIT Press, 2009.

[74] D. F. Wamala, "The ITU National Cybersecurity Strategy Guide," ITU, Geneva, 2011.

[75] "Cyber Security Strategy for Germany," Federal Ministry of the Interior.

[76] "Harmonizing Cyberlaws and Regulations: The experience of the East African Community," in *United Nations Conference on Trade and Development* , Geneva, 2013.

[77] ENISA, European Union Agency for Network and Information Security, [Online]. Available:https:/www.enisa.europa.eu/about-enisa. [Accessed 24 March 2019].

[78] M. Kerttunen, "APNIC," 04 April 2019. [Online]. Available: National Cybersecurity Strategies: Commitment to Development. [Accessed 15 April 2019].

Appendix 1 – Online Questionnaire

National Cyber Security Strategy

The public and other stakeholders are invited to participate in a questionnaire as part of the research with a theme National Cyber Security Strategy: An Application perspective to Ethiopia. The Questionnaire is totally anonymous.

1. Choose the one which best describes you and your work profile? *Mark only one oval.*

   ○ Private Sector

   ○ Civil Society

   ○ Government or Public Sectors

2. What describes your level of reliance on Information Communication Technologies (ICTs)

   ○ Low

   ○ Medium

   ○ High

3. Have you experienced any Cybersecurity breaches to your network or system? *Mark only one oval.*

   ○ Yes

   ○ No

   ○ Maybe

4. If your answer is yes. Please indicate all of the cyber security incidents (cybercrime) committed against your organization?(Select all Applicable)
   Check all that apply.

   □ Malware

   □ Website Defacement

   □ Password-Based Attack

□ Phishing

□ Session Hijacking and Man in the middle attacks

□ Cross-site Scripting (XSS)

□ Denial of Service (DOS)

□ Other: ____________________

5. Where is the source of the threat (Cybercrime)? *Mark only one oval.*

○ Insider

○ Outsider

○ Both

○ Not Sure

13. Do you think there are adequate Cyber security institutions and measures currently in place at the national level in Ethiopia?
Mark only one oval.

○ Yes

○ No

○ Maybe

14. Do you know the existence of National Information Security Policy in Ethiopia? *Mark only one oval.*

○ Yes

○ No

15. Does your organization report cyber security incident (cybercrime) to law enforcement?
Mark only one oval.

○ Yes

○ No

16. How do you describe the level of reporting mechanism of cyber incidents in Ethiopia? *Mark only one oval.*

○ Very effective

○ Not effective

○ No reporting mechanism is established

17. Does your organization have a budget for Cybersecurity?

Mark only one oval.

○ Yes

○ No

18. Which public infrastructure and online services do you think the Government should protect in terms of Cyber security? Please tick all applicable options

Check all that apply.

□ Electricity

□ Water and Sewerage

□ Banking Service

□ Health Service

19. Do you think the Government of Ethiopia currently has in place adequate policies or laws dealing with Information sharing, Data protection, and Privacy?

Mark only one oval.

○ Yes

○ No

20. Do you have any other general comments and or observations in relation to Ethiopian cyber security readiness/ policies? Please state your views.

____

____

____

____

____

Appendix 2 – Respondent Observation

Do you have any other general comments and or observations in relation to Ethiopian cyber security readiness/ policies? Please state your views.

- Ethiopian Cyber Security policy should be improved from the protection system to development, research and respond cyber-attack action system.
- The recent initiatives of the Ethiopian government with regard to adopting cyber Security policies and building the concerned institutions are promising. But most of the high level leaders of the organisation lack awareness and attention on cyber-security. Because of this, the adopted IT security standards not adhere strictly. The other problem is the lack of technically well-equipped personnel.
- The government shall improve security as we go to the global cyber market and the virtual economy.
- The started cyber security system shall be strengthened.
- It is a serious issue should be available, but in Ethiopia, it's not concerned in ma opinion should be focused on the policy
- Strict policy needs to be designed and implemented.
- As an Ethiopian cyber security professional, i would say the country is barely prepared for the most common and silliest attacks out there. I would say Ethiopia is one of the most vulnerable and under prepared countries in this frontier, both at the organizational level (policies) and technical capabilities of handling incidents (technical skills).
- As far as my knowledge is concerned, Ethiopia has no clear cyber security policy. So, you have to do your best on it for your country.

Appendix 3 – Interview Questions

1. What is the purpose of an NCSS & who should participate in the development of National Cybersecurity Strategy?
2. What are the challenges in developing NCSS?
3. What is defined as Critical infrastructure and why?
4. How does NCSS reflect countries political, strategic objectives, and key principles?
5. What, how, from whom you have received political guidance?
6. What other national strategies or programs have guided your work?
7. What national or universal values and norms have guided your work?
8. Have you used ‘international’ guidance, models or templates in national strategy formulation? In your opinion, what is the value of these guidelines?
9. What other national strategies, domestic guidelines or programs have guided your work?
10. What national or universal values and norms have guided your work?
11. Have you used ‘international’ guidance, models or templates in national strategy formulation? In your opinion, what is the value of these guidelines?
12. Do you think that countries should have their own NCSF and how often do you think NCSS have to be reviewed (revised)?
13. What is the need for having a public-private partnership in national cybersecurity strategy?
14. Have you participated in cyber capacity-building programs? In your opinion, what is the value of cyber capacity-building in the context of national strategy formulation?
15. What additional information on cyber security strategies would you like to provide or expound upon before ending the interview?