The Federal Democratic Republic of Ethiopia

National Cyber Security Policy and Strategy

October 2021
Addis Ababa, Ethiopia

Table of Contents

Definition of Terms

In this policy and strategy, unless the context otherwise requires:

Critical Information Infrastructures mean physical and digital assets, networks, services and information systems that, if an attack is inflicted on these infrastructures, would have a serious impact on public security and national interests of the country.

Cyberspace means a virtual space that comprises interconnected information, information infrastructure, information systems, and human resource that turns information into knowledge and use it, and the institutional and social culture.

Digital Identity means an online or networked identity adopted or claimed in cyberspace by an individual, organization, or electronic device.

Digital Identity Protection means protecting the confidentiality and the integrity of information owned by the individuals, the citizens, or the institutions in cyberspace as well as protecting the common identity; it also includes preventing unauthorized access.

Cyberbullying means any type of intimidation and similar acts committed through the internet and related electronic means.

Cybercrime means a crime that is committed using information communication technologies and systems, especially the Internet.

Cyber-attack means unauthorized access to data, data theft, spreading of malware, psychological warfare, and other cyber-attacks.

Cyber Security Policy means a course of action to govern and manage cyber security.

Cyber Security Strategy means how the cyber security policy's mission, objectives, and goals should be achieved; it is a calculated plan, method, and action to achieve the desired result.

Data Privacy means the right to personal data privacy and protection which includes but is not limited to, protection against unauthorized access to personal information, against passing the information to the third party without the owner’s permission, against compromising the integrity of the information.

Acronyms

ICT	Information and Communication Technology
INSA	Information Network Security Agency
Ethio-CER^{2}T	Ethiopian Computer Emergency Readiness and Response Team
FDRE	Federal Democratic Republic of Ethiopia
NCSPS	National Cyber Security Policy and Strategy
R & D	Research and Development

Introduction

Our world is experiencing rapid and complex changes with the advancement of technological and scientific innovations of this 21St century. Particularly, the appearance of cyberspace as one domain has transformed our world into a small village heralding globalization. Cyber, which is primarily based on the Internet, enabled the world to be interconnected so that any information from anywhere in the world can be accessed in seconds, enabled the connection between people not to be limited in space and time, availed a fast data exchange, fundamentally altered the lifestyle of a human being by changing the social, economic and political realities, and created a new chapter in the life of human being.

Hence, it is now becoming a reality that it is not possible to remain out of cyberspace; without cyber, it is now almost impossible to survive as a sovereign country let alone become competent. A country and people that cannot be competent enough in cyberspace cannot maintain its sovereignty in its totality.

Cyberspace is an arena of high-security threats and risks. Especially, as cyberspace is an arena engulfed with responsibilities of protecting the cyber sovereignty, ensuring the privacy of individuals, and of facing the paradox attached to the advancement in ICT, ensuring the security of this space is becoming the challenge of all nations. Thus, the countries of the world are giving attention to running the cyber security issues in parallel with the rapid development in ICT to exploit the economic, social, and political benefits and opportunities that the new space availed. Cyber security has become high on the agenda from technologically advanced to developing nations.

Consequently, it is a challenging assignment for countries to ensure cyber security. As ensuring cyber security became the question of survival not that of a choice, international institutions and countries of the world are striving 24/7. As a result, many countries formulate policies to make sure that cyber security is ensured.

Ethiopia, like any other country, is exploiting the opportunities and facing security challenges that are parallel to the fast-growing ICT infrastructure. In line with this, the country's limited resources, technology dependence and high vulnerability, low cyber security awareness, lack of expertise, and underdeveloped research work pose a security risk.

Therefore, to take full advantage of the opportunities the sector presents and to ensure its security, it is necessary to develop an up-to-date policy and strategy. As a result, this National Cyber Security Policy and Strategy (CSPS) is formulated by amending the previous National Information Security Policy that has been effective since 2011.

Part One

Policy and Strategy Need, Vision, Mission, and Objectives

1.1. The Need for the NCSPS

The NCSPS has been developed as it is deemed important because of the following reasons:

1. As the overall situation and behavior of cyber security has changed with the development of ICT, we have reached the point where it is progressively challenging to properly protect the sovereignty and security of a country. Consequently, Ethiopia is cognizant that it needs an up to date cyber security policy and strategy to protect the security of the complex, dynamic, unpredictable, and high-tech prone cyber, to be able to take advantage of the enormous opportunities that cyber brings with it, and to mitigate the risks therein;
2. As cyberspace is gaining a big share in Ethiopia's socio-cultural, political, economic, and security arena, and creating a tangible influence than ever before, it is important to set cyber security policy directions and strategies that consider the existing situation;
3. Due to the increased risks, vulnerabilities, and attacks to cyber security as the result of the expansion and digitalization of key infrastructures and systems by which the country's information is stored, analyzed, and disseminated;
4. For cyber security by its very nature is not the role and responsibility exclusive to government, there is a need to increase coordination and partnership between public and private institutions and other stakeholders;
5. Given the multifaceted potential of the private sector in cyber security as seen in the realities of the rest of the world and its growing involvement in key infrastructures in our country, it is necessary to administer the role of the private sector with that of the government institutions in a reasonable and complementary fashion;
6. Considering the apparent global cyber security threats and vulnerabilities, it is deemed necessary to know and use the up to date technologies, to establish legal and regulatory frameworks, to build research and development capacity, to raise awareness; and to state policy directions and strategies that take into account the existing and imminent cyber security threats, and to establish a monitoring and evaluation system;

1.2 Fundamental Assumptions

1. Government Leadership Commitment

The government gives strategic directions for the coordinated distribution of resources and capacities needed for the proper implementation of the NCSPS.

2. Shared Responsibility

As cyber security is the concern of multiple stakeholders, citizens, the government, the private sector, and other concerned bodies need to implement the NCSPS with shared responsibility and a strong sense of ownership, integration and collaboration.

3. The Rule of Law

To ensure the constitutional rights, freedom, and equitable benefits of citizens; to create reliable cyberspace, and to guarantee that the task of ensuring cyber security and the rule of law among the highly interconnected cyber society is to be taken as a key role as it is a reality in the physical world.

4. International Cooperation and Partnership

As cyber security threats, vulnerability and attacks have a cross-border nature, it requires building strong international cooperation and partnership.

5. Ethiopian Values

This National Cyber Security Policy and Strategy will be implemented in a manner that respects the values of Ethiopians.

1.3 Vision

To see a globally competent and resilient national cyber security capability;

1.4 Mission

To protect national interests by building a self-reliant cyber security capability that enables to safeguard the country's information and key information infrastructure from cyber-attacks;

1.5 Objectives

1. To build resilient cyber security capability that monitor, detect and warn threats and vulnerability; and that prevent and give quick response to cyber attacks;

2. To enable cyber security to play a role in the protection of citizen's privacy, human rights, democratic rights, and in the assurance of sustainable peace and development in its process and end;
3. To establish strong national, regional, continental, and international partnership and collaboration on cyber security;
4. To build indigenous technological capabilities and deploy systems that sustain key infrastructure and information resources through the R&D which is up to the international standard;
5. To create an aware society that uses cyber with knowledge and reason through building a local cyber security culture;

1.6 Principles

1. **Accountability**

All public and private institutions have the accountability to protect their information and information infrastructure and systems; to ensure the security of their cyber products and services.

2. **Resilience**

It is incumbent to affirm cyber security by withstanding the challenges in cyberspace, by being resilient, and by remaining strong and more agile.

3. **Sovereignty-Centric**

The country should make sure that its cyber sovereignty and national interests are intact in all its international cooperation, negotiations, and agreements in the field of cyber security.

4. **Coordination and partnership**

As the task of ensuring cyber security requires the participation of all concerned bodies, the public and private institutions, and other stakeholders need to work in coordination and partnership.

5. **Global Compliance**

Since the task of securing the cyber is practiced in a global space, it should be done by international laws, principles, and agreements.

6. **Balancing privacy and security**

The NCSPS will be implemented by maintaining the balance between the protection of cyber security and the rights and privacy of individuals.

1.7 **Scope of the NCSPS**

The NCSPS applies to all public, private and other institutions in the country and focuses on ensuring the security of the information, key information infrastructures and systems of these institutions, and safeguarding the security of any personal data of individuals.

Part Two

Focus Areas and Strategies

2.1. Policy Issues

It is becoming a challenging issue to maintain the sovereignty of states in the cyber world. Especially, in cyberspace that has a global nature, the cyber sovereignty of a state which has not built a competent capability will be under question in one way or another. This happens because of the reason that the leading states in cyber technology do not easily transfer the technology to other states and for the reason that the technology creates a convenient environment to put other states under their influence. As a result of this, those states which are lagging in technology will highly be vulnerable. On the other hand, as avoiding the cyber world is not an option, countries have become part of this globalization. Thus, in addition to building the technological capability in the area, countries strive to ensure cyber security through establishing a regulatory mechanism.

The fact that Ethiopia is a developing country cannot immune it from the vulnerability that comes with cyber and cyber technology. Hence, it needs to set in place a regulatory mechanism in addition to advancing its cyber defense capability by arming itself with cyber security technology internally through research and development schemes or procurement. In this process, it needs to build a knowledge-based system by understanding the paradoxes in the cyber world. Therefore, considering the global and national cyber security reality on the ground, major policy issues have been identified.

Accordingly, the NCSPS comprises seven major policy focus areas. These are Legal and Regulatory Framework, Awareness, Capacity Building, Research and Development, Digital Identity and Personal Data Protection, Key Information Infrastructure Protection, and International and National Cooperation.

2.2. Legal and Regulatory Framework

2.1.1. Policy Statement

It is important to develop and implement up-to-date legal and regulatory frameworks that are consistent with the reality on the ground to reduce the progressively increasing cyber security vulnerability and threat, defend against attacks, and hold perpetrators accountable.

Therefore, it is important to develop and implement cyber security laws, policies, strategies, standards, and other frameworks to prevent cybercrime, cyber terrorism, cyber espionage, and other illegal activities in the country. Thus, the following legal and regulatory objectives, strategies, and tactics are designed and to be implemented.

2.1.2. Goals

The goal of the legal and regulatory framework shall be:

1. Developing and continuously revising cyber security legal and regulatory frameworks that are consistent with international laws and standards adopted by the country and making continuous improvements to them;
2. Building the capacity of law enforcement entities to prevent cybercrime, cyber terrorism, cyber espionage, and other illegal activities;
3. Establishing a regulatory system that ensures the locally produced and imported cyber security products and services, and the installation of key infrastructure that meets the national cyber security requirements.
4. Establishing up to the standard legal and regulatory frameworks for data collection, analysis, dissemination, usage, storage, and disposal to increase public trust in the country's cyber security capabilities;

2.1.3. Strategies and Tactics

1. Developing and improving binding and up-to-date substantive and procedural legal and regulatory systems that are compliant with national cyber security conditions;

    Tactic One: Cyber security laws, policies, standards, and systems to be implemented by government and key private institutions will be developed;

    Tactic Two: All stakeholders will be involved in the development process of cyber security legal and regulatory frameworks to increase their acceptance and enforcement;

    Tactic Three: Controlling technologies are used to ensure accountability in cyber security before the law;

2. Producing competent legislators, law enforcement, and judiciaries on cyber security legal and regulatory frameworks and building their capacity continuously;

Tactic: To enforce legal and regulatory frameworks of cyber security the capacity of investigators, prosecutors, judges, and other judicial bodies will be built continuously through education, training, consultative forums, conferences, and the like;

3. Developing quality control and other regulatory standards related to the provision of cyber security products and services, and the disposal of products that are out of service;

   Tactic: Quality and reliability check on the domestic and imported cyber security products will be conducted; the capacity of the implementers will be built continuously;

4. Monitoring and prosecuting illegal cyber activities to ensure the confidentiality, integrity, and availability of information, and to deter other intentions;

   Tactic: Notification of legal cases on cyber security will be available for the public;

2.3. Cyber Security Awareness

2.3.1. Policy Statement

As cyber security is the result of technology, process, and human interaction, it is important to raise cyber security awareness to prevent cyber security threats, vulnerabilities, and attacks that may occur especially due to lack of knowledge and attitudes, and performance gaps of public and private institutions and citizens. Therefore, the government gives focus to the following goals, strategies, and tactics so that knowledge-based information-sharing culture concerning information value and cyber attacks of the country will be built, and attitudinal and behavioral changes will be realized.

2.3.2. Goals

The goals of cyber security awareness shall be:

1. Building the knowledge and attitudes of public and private institutions, professional and civic associations, and citizens on cyber security;
2. Reducing cyber security vulnerabilities and threats, and preventing cyberattacks that may arise from carelessness, ignorance, and negligence;
3. Raising public awareness and bolstering a national cyber security culture to reduce cyber security vulnerabilities and threats, and to prevent cyber attacks;

2.3.3. Strategies and Tactics

1. Establishing institutional structures and systems to improve cyber security awareness;

   Tactic One: Cyber security awareness scheme will be set to the society through stretching the structural accessibility of the institutions involved in cyber security

   Tactic Two: Awareness-raising activities are performed using technologies that give a quick response to cyber security incidents.

   Tactic Three: Cyber security awareness clubs will be established in educational institutions;

2. Developing up to standard national cyber security awareness frameworks and programs to be implemented in public and private institutions;

   Tactic One: There will be situational and continuous cyber security forums, discussions, and similar awareness-raising platforms on all institutions, but with special focus on critical infrastructures in the country;

   Tactic Two: National cyber security awareness campaigns will be carried out;

3. Equipping the mass media with systems that enable them to raise and develop awareness on information value and basic cyber security awareness;

   Tactic One: Various up to date cyber security programs will be developed and communicated through mass media to raise public awareness and understanding;

   Tactic Two: The media, private institutions, civic institutions, and other bodies that work on cyber security will be commended and motivated.

2.4. Capacity Building on Cyber Security

2.4.1. Policy Statement

The lack of trained human resources and lack of strong cyber security systems and institutional structures in our country has contributed to the cyber security capacity being at a low level. As a result, citizens, government, and private institutions became vulnerable to various forms of attacks and deprived of reaping the benefits cyberspace provides sufficiently.

Therefore, as the ability of the government to be able to build a strong cyber security capability has a significant contribution to the economical, political, and social development, and transformation of the country, the government has set out the following objectives, strategies, and tactics to build a strong cyber security culture among the community, to expand education and training programs, to build institutional capacity and establish working systems, and to build resilient and flexible cyber security capabilities at the national level.

2.4.2. Goals

The goal of building cyber security capacity shall be:

1. Building a capacity and setting a structure that enables to detect and respond to cyber security threats, vulnerabilities, and attacks;
2. Strengthening the cyber security capacity of public, private, and higher education institutions;
3. Producing competent cyber security experts and leaders at the national level;

2.4.3. Strategies and Tactics

1. Establishing up to standard cyber security education and training program in the country by developing cyber security curriculum for primary, secondary, and higher education institutions;

   Tactic One: Cyber security education will be included in the education policy of the country;

   Tactic Two: Up to date educational and training certification will be provided to professionals to enhance their cyber security capabilities;

   Tactic Three: A standard of competency for cyber security professionals will be set;
2. Developing efficient and capable institutional structures and systems that enable the cyber security capacity building scheme;

   Tactic One: Public and private institutions will implement systems to facilitate cyber security knowledge transfer;

   Tactic Two: Structures for flourishing cyber security knowledge and skills will be established and implemented by public and private institutions;

Tactic Three: Institutions that train, hunt, and enhance talents in cyber security will be established and the existing ones will be strengthened;

3. Establishing an effective cyber security knowledge management and distribution system at the national level;

   Tactic One: Best practices, experiences, and knowledge sharing platforms on cyber security will be set up among the government, private, and higher education institutions;

   Tactic Two: A permanent exhibition will be held and libraries will be established to enable cyber security knowledge sharing;

4. Producing an energetic and competent workforce through creativity, talent-based programs that safeguard national interests;

   Tactic One: A competency building work will be done on experienced and newly recruited professionals of key information infrastructure institutions by giving special attention to their personality and talent;

   Tactic Two: International forums to develop creativity and talent will be formed in coordination with institutions engaged in cyber security;

2.5. Cyber Security Research and Development (R & D)

2.5.1. Policy Statement

As cyberspace, by its very nature, is very complex, dynamic, and unpredictable, it is important to study challenges associated with emerging technologies and propose solutions; it is also vital to conduct R&D that helps develop knowledge, skill, and innovations in the area. In addition to this, it is imperative to develop cyberinfrastructures and technologies, to expand technology transfer and innovations, and to conduct R&D that has a national and international impact at a different level. Consequently, the government strives to flourish indigenous research capacity in the area, to build cyber security industry through organized research and development, and to protect intellectual property rights. To this end, the government identifies the following goals and strategies and works to achieve them.

2.5.2. Goals

The goals of Cyber security R&D shall be:

1. Make the cyber security products and services that ensure the security of critical information infrastructures based on R&D;
2. Identify the cyber security threats, vulnerabilities, and attacks through research and provide solutions;
3. Build R&D capacity based on indigenous knowledge and innovation to ensure cyber security;
4. Build an internationally competent and integrated national cyber security R&D culture;

2.5.3. Strategies and Tactics

1. Backing the indigenous cyber security products and services with research and development;

   Tactics one: Activities that enable to lead cyber security industry through research and development will be carried out;

   Tactic two: A research-based indigenous cyber security technology that protect key infrastructure from attack will be made accessible to the users;

   Tactic three: Various incentives to motivate the innovation of new products and services that promote cyber security research will be provided;

   Tactic four: R&D programs that produce value-added products and services by adopting new technologies will be designed;

2. Expanding programs that enable to build R&D capacity on cyber security by creating cooperation and partnership between higher education institutions and the industry;

   Tactic One: Knowledge, skill, experience, and technological capacity that enable accomplish R&D tasks will be built;

   Tactic Two: Cyber Security Center of Excellence in various research institutions, security agencies, and higher education institutions will be established, if deemed necessary;

   Tactic Three: Knowledge and experience sharing forums, conferences and other events that enable to build R&D capacity among the actors in the cyber space will be held;

   Tactic Four: R&D activities will be carried out by the government and private institutions in coordination with higher educational institutions;

Tactic Five: A standard that determines the capability and quality of the bodies involved in the cyber security R&D capacity building will be set;

3. Supporting R&D that enables to reduce threat and vulnerability, to defend and respond to attacks, and to build resilience continuously;

   Tactic One: A continuous R &D support will be provided to protect the vulnerability and attacks facing the key information infrastructures;

   Tactic Two: A conducive environment that enables the private sectors to involve in the cyber security R&D programs of the country will be created;

4. Promoting R&D in cyber security issues that can be a national priority as actual and potential cyber threats;

   Tactic One: R &D activities will be performed by giving special attention to threats that come with the development of the technology and that may cause damage to the country's security;

   Tactic Two: A resilient national cyberspace and cyber security industry development will be supported with R &D;

2.6. Digital Identity and Personal Data Protection

2.6.1. Policy Statement

If digital identities and personal data are not well protected, it will lead to cyber-attacks on citizens, identity-based attacks, and deviance from the culture of the society and values resulting in compromising the privacy and human rights of citizens. Hence, the government sets the following goals and strategies to prevent psychological attacks on citizens, raise public awareness, reduce the risk and vulnerability of digital identity and personal data, and ensure the security of the information infrastructures used by citizens.

2.6.2. Goals

The goal of digital identity and personal data protection shall be:

1. Ensure a credible digital service and personal data protection for citizens;
2. Protect national values and norms from cyber security threats, vulnerabilities, and attacks by enhancing the constructive role that cyber can play in educating children;
3. Protect and minimize gender-based cyber-attacks, sexual harassment, cyber bullying and psychological influence that may happen in cyberspace;

4. Protect religious, ethnic, and other identity based digital attacks;

2.6.3. Strategies and Tactics

1. Developing binding legal frameworks for the protection of digital identity and personal data, and establishing technology-based systems;

    Tactic One: Frameworks to ensure the security of personal data will be developed and implemented in a coordinated manner;

    Tactic Two: A technology-based cyber security regulatory system that do not compromise data privacy will be implemented;

    Tactic Three: personal data collection, process, and regulation directives will be developed;

    Tactic Four: There will be a balanced approach towards personal data protection in the due process of ensuring cyber security;

2. Establishing a system to ensure the security of government electronic services;

    Tactic One: A personal data protection agreement will be reached between the individuals and institutions regarding the rights and obligations of individuals on their data collected, processed, stored, and used**;**

    Tactic Two: Institutions will be overseen to include in the cyber security directives and other guidelines they formulate about the protection of the right to the privacy of the individuals.

    Tactic Three: Continuous monitoring and analysis will be carried out in every institution regarding the personal data protection of individuals;

3. Establishing a system to prevent religious and ethnic-based derogatory comments and similar identity-based hate speech using the cyber;

    Tactic One: Regulations and operational procedures that prohibit hate speeches and other related issues; and that promote the proper use of cyber security will be implemented;

    Tactic Two: Regulatory technologies to detect and protect cyber-based hate speeches and fake news will be applied;

4. Developing frameworks and establishing operational procedures that protect good personality and security of the children in cyberspace;

Tactic One: Follow up procedures to prevent violation of digital rights of children will be in place;

Tactic Two: Institutions perform their tasks by respecting the children's digital rights;

Tactic Three: Controlling mechanism to protect children from children focused anti-culture contents in cyberspace will be in place;

5. Supporting institutions to develop programs that protect the digital identity of women and children;

Tactic One: Public campaigns will be organized to strengthen the protection of digital identity and personal data of women and children;

Tactic Two: Discussion forums on digital privacy protection of women and children will be facilitated;

Tactic Three: Actions to reduce cyber-based psychological attacks on women will be taken;

2.7. Critical Information Infrastructures Protection

2.7.1. Policy Statement

As information is becoming a valuable resource, it is important to protect critical information infrastructures from cyber-attacks, reduce cyber threats and vulnerabilities, and be resilient. As it is important to protect critical information infrastructure to ensure cyber security and to uplift trust, the government gives due attention to the sector.

Therefore, to prevent cyber incidents and attacks that may target critical information infrastructures, and to properly govern and manage the country's economic, social and political issues in coordination and partnership with the private sector, the government will work by setting the following objectives, strategies, and tactics.

2.7.2. Goals

The goals of critical information infrastructures protection shall be:

1. Develop the capacity to identify, prevent, and respond to cyber threats, vulnerabilities, attacks, and damages to critical information infrastructures and institutions;
2. Ensure the security of imported and local critical information infrastructure products and services;
3. Create coordination and partnership between the public and private sectors to provide special protection for critical information infrastructures;

2.7.3. Strategies and Tactics

1. Building institutional structures and capacity; and establishing operational procedures that enable to identify, defend and respond to potential threats, vulnerabilities, attacks, and damages to critical information infrastructures;

   Tactic One: A coordinated national cyber security system will be implemented to ensure the cyber security of critical information infrastructure withing public and private institutions;

   Tactic Two: An entity that can detect and give a rapid response to attacks on critical information infrastructures will be established;

   Tactic Three: National critical information infrastructure security governance system will be established; it will be updated continuously in compliance with new developments;

2. Building capacity to develop up to the standard control systems for preventing attacks on critical information infrastructure;

   Tactic One: Public and private institutions will implement international standards and nationally contextualized cyber security laws, policies, standards, and frameworks;

   Tactic Two: Critical infrastructure sectors will be required to design and incorporate programs that address international issues which comply with the country's information security standards and operational procedures;

   Tactic Three: Education and training on current issues will be conducted, and discussion forums will be organized for stakeholders to detect, prevent and respond to threats, vulnerabilities, attacks, and damages to critical information infrastructures;

Tactic Four: Build a capacity to produce and supply indigenous products and services that are used to secure critical information infrastructures;

3. Developing secured information infrastructure products, services, communication systems, reliable networks, and control systems technology;

   Tactic One: Standards will be employed for ensuring the security of critical information infrastructures, ICT products, and services ;

   Tactic Two: Information and information infrastructure vulnerability assessment, penetration testing, and security audits will be conducted, and immediate remedial action will be taken at any time;

4. Enhancing the role of public and private institutions, and other concerned stakeholders to provide special protection for critical information infrastructures;

   Tactic One: By classifying critical information infrastructures persistently, criteria for setting their roles and responsibilities will be prepared and implemented;

   Tactic Two: A 24/7 physical and virtual protection is provided for critical information infrastructure and systems;

   Tactic Three: The duties and responsibilities of all stakeholders will be identified to provide special protection for critical information infrastructures;

2.8. National and International Cooperation

2.8.1. National Coordination and Partnership

2.8.1.1. Policy Statement

Cyber security attacks are so complex, unpredictable, dynamic, and borderless that cannot be dealt with government or a limited number of institutions alone. Hence, establishing national coordination and partnership to ensure cyber security, and also tackling cyber security threats should be a shared responsibility of all stakeholders. In particular, the development of cyber security products and services requires the active participation of the private sector. The private sector has been making progress in the country's information technology industry development. On the other hand, though the private sector can play a key role in accelerating the cyber security efforts of the country, as of now, the participation of the sector in the area is limited. To change this, the government encourages the involvement of the private sector in the development of the cyber security industry.

Therefore, to ensure cyber security at the national level, the government mobilizes and makes use of national capacity and enhances the role of the private sector. To this end, it sets the following objectives and strategies and implements them.

2.8.1.2. Goals

The goal of national coordination and partnership shall be:

1. Establish and strengthen coordination and partnerships among government, private sector, and relevant stakeholders to ensure national cyber security;
2. Enable local private sectors that are engaged in cybersecurity production and service delivery to be competitive in the local and international market;

2.8.1.3. Strategies and Tactics

1. Establishing a system of coordination and partnership between public and private sectors that play a key role in national cyber security;

   Tactic One: A system that governs cyber security coordination and partnership will be established and implemented;

   Tactic Two: National cyber security platforms that strengthen coordination and collaboration will be formed; and regularly held at the national level.

2. Enabling citizens, the private sector, civic societies, and other stakeholders to play their part in defending against cyber attacks;

   Tactic One: Clarity on roles and responsibilities will be created among stakeholders;

   Tactic Two: There will be experience sharing and knowledge transfer scheme among cyber security stakeholders;

3. The Ethio-CER^{2}T will be used as a bridge among all public and private institutions for cyber security;

   Tactic One: Both public and private institutions will be enabled to have a Computer Emergency Response unit for experience sharing scheme on cyber incidents.

   Tactic Two: A Computer Emergency Response units of both public and private institutions will be coordinated with the national CER^{2}T;

4. Establishing a system of coordination and partnership that will increase and strengthen the participation and contribution of the local private sector in the development of cyber security industry;

   Tactic One: Programs will be developed and implemented to help create new institutions and strengthen the existing ones;

   Tactic Two: An incentive system will be established for entities that produce cyber security products for the benefit of the public;

   Tactic Three: A supporting mechanism will be in place that enables up to the standard cyber security products and services to compete in the domestic market;

   Tactic Four: Due focus will be given to the private sector to make it competitive in international markets;

2.8.2. International Cooperation

2.8.2.1. Policy Statement

To mitigate threats and vulnerabilities, and to defend against attacks that may arise from the dynamic and borderless nature of cyberspace, countries formulate and implement different policies, strategies, standards, practices, and perspectives. Though this is a step forward, if there is no cooperation among countries, it will be difficult to maintain security at the required level. As a result, to defend against cyber security threats, vulnerabilities, and attacks, and enhance cyber security situations, and create secured cyberspace, countries opt for international cooperation. Recognizing this fact, the government has set international cooperation as a policy focus area to enable knowledge and technology transfer and the prevention of organized cybercrime such as cyber terrorism, cyber espionage, and other transnational cybercrimes.

2.8.2.2. Goals

The goal of international cooperation shall be:

1. Create cooperation to prevent cybercrime, cyber terrorism, cyber espionage, and similar cross-border security threats;
2. Make international cooperation on cyber security to be part of the country's cyber diplomacy;
3. Encourage and promote bilateral and multilateral cyber security agreements;

2.8.2.3. Strategies and Tactics

1. Establishing a system of cooperation to address legal issues related to cybercrime, cyber terrorism, cyber espionage, and similar cross border cyber security threats;

    Tactic: International cooperation and partnership agreements will be made on cyber security;

2. Establishing international cooperation which is based upon technical and legal frameworks to prevent cross-border cybercrime, cyber terrorism, cyber espionage, and similar attacks;

    Tactic One: Experience sharing mechanisms with various countries and international organizations for defending cyber-attacks will be facilitated;

    Tactic Two: There will be information sharing and technical cooperation and assistance with other countries;

    Tactic Three: Cyber security will be an integral part of foreign policy;

3. Establishing a system to speed up international experience sharing and knowledge transfer;

    Tactic One: Studies that enable actively participate in international, continental, and regional agreements and negotiations will be conducted;

Tactic Two: A conducive environment will be created for private and public institutions to strengthen their cyber security ties with other governments and private institutions;

Tactic Three: International training will be facilitated to create a competent human resource on cyber security issues;

4. Creating compliance between cyber security laws and policies of the country with international legal frameworks and standards;

Tactic One: There will be active participation in international cyber security cooperation forums in line with the need of the country;

Tactic Two: Awareness will be created on the relevant international laws signed and ratified by the country, and on the trends of the sector;

Part Three

Policy and Strategy Implementation Framework

3.1. General Overview

It is important to identify the role and responsibility of the concerned institutions, establish the necessary new structures, establish the monitoring and evaluation systems, and point out directions to implement this NCSPS. As cyber security is inherently complex and highly dynamic, it is difficult for any country to overcome the challenges alone. It is, therefore, important to work in collaboration and partnership with a variety of stakeholders. Hence, for the NCSPS to be effective, it requires the engagement of the government, the private sector, the educational and research institutions, the civil society organizations, and other national and international stakeholders. To this end, the government provides strategic leadership to implement the policy.

3.2. Institutional Structure

To ensure cyber security in our country, it is necessary to create strong institutions and to strengthen the existing ones. Cognizant of this fact, the government has established INSA and Ethio-CER^{2}T to protect and respond to cyber attacks targeting the country and its key infrastructures.

To ensure cyber security, it is important to cooperate and work in partnership with various national institutions. To make this collaboration and partnership effective, National Cyber Security Council, which comprises the concerned government, private, and other stakeholders, will be established. The government may establish new institutions and task forces at the national and sectoral levels to facilitate the implementation of the policy and strategy, or assign additional responsibilities for existing institutions. To make the institutional structure helpful to the implementation of this NCSPS, it will be developed in a manner that takes into account the private sector.

3.3. Roles and Responsibilities of Stakeholders

It is incumbent on all government institutions, on private sectors with key information infrastructures, and on other concerned stakeholders to implement this NCSPS. They also have the responsibility for designing and implementing cyber security programs in consistence with this NCSPS and international standards.

3.4. **Monitoring and Evaluation**

To measure the effectiveness of the NCSPS at all levels and to realize the execution process, a monitoring and evaluation system which includes the following key issues will be in place:

1. An action plan for the implementation of the policy and strategy will be prepared by INSA; the Cyber Security Council will play its role in the implementation.
2. A monitoring and evaluation system shall be established to ensure that public and private institutions and other stakeholders carry out the relevant activities specified in the NCSPS, perform activities listed in NCSP implementation frameworks, establish the necessary institutional structure, and allocate the required budget and resources;
3. For the implementation of NCSPS, data collection, organization, and analysis activities will be carried out and a reporting system will be established with coordination of INSA;
4. An annual stakeholders meeting will be organized by INSA to evaluate the implementation of the NCSPS;
5. Based on the results of NCSPS monitoring and evaluation, directions to develop other necessary frameworks and, if need be, to revise the NCSPS will be given.

3.5. **Legal Issues**

1. This NCSPS shall be implemented upon approval by the House of Representatives;
2. The NCSPS shall legally be binding on all parties directly or indirectly referred to in this document;
3. Legislation may be enacted to hold those who fail to implement this NCSPS accountable;

3.6. **Financial Issues**

1. The budget required to implement the NCSPS and to carry out other related activities shall mainly be allocated by the government;
2. The budget allocated for the implementation of the NCSPS shall be run following the monitoring and evaluation system set in the policy and strategy and by the decision of the body endowed with a legal responsibility to oversee the NCSPS.

3. Projects and programs designed to implement the policy goals, strategies, and tactics will be carried out in collaboration with the relevant bodies as needed;

3.7. **Success Indicators**

1. Stable socio-cultural, economic, and political conditions as a result of reduced cyber security risks, threats, vulnerabilities, and attacks;

2. Developed Cyber security capacities and systems at the national, sectoral, and institutional levels;

3. The delivery of cyber security products and services through national capacity;

4. An aware society that uses the cyber safely; and a built national cyber security culture;

5. A built cyber security industry with the participation of the private sector;

6. The strengthened and tangible cyber security partnerships and collaborations at the international, regional, and national levels resulted in a contribution to the national interest.

3.8. **Revision**

The NCSPS may be revised as the result of the impact that the political, economic, social, and technological changes in the country bring on the process of ensuring cyber security; when new needs arise with the development of the role and responsibilities of public and private institutions in the sector; as well as when the direction is given based on the findings of the NCSPS monitoring and evaluation. Based on the above-mentioned perspectives, the NCSPS will be revised in five years beginning from the date of ratification. By the direction set forward by the Cyber Security Council considering the findings of the monitoring and evaluation result, INSA takes the responsibility of revising the NCSPS.