THE REPUBLIC OF UGANDA

NATIONAL CYBERSECURITY STRATEGY

TABLE OF CONTENTS

ABBREVIATIONS

Acronym	Explanation
3i	Inclusive Internet Index
4IR	4th Industrial Revolutions
AFRIPOL	African Union Mechanism for Police Cooperation
APSA	African Peace and Security Architecture
AU	African Union
AUCSEG	African Union Cybersecurity Expert Group
CCI	Commonwealth Cybercrime Initiative
CERT	Computer Emergency Response Team
CERT.UG/CC	Uganda National Computer Emergency Response Team and Coordination Centre
CI	Critical Infrastructure
CSIRT	Computer Security Incident Response Team
EDGI	E-Government Development Index
FIRST	Forum of Incident Response Teams
GDP	Gross Domestic Product
GFGE	Global Forum on Cybersecurity Experts
GGE	Group of Government Experts
GNI	Gross National Income
GoU	Government of Uganda
ICT	Information and Communication Technology
IDI	ICT Development Index
INTERPOL	International Criminal Police Organization
ITU	International Telecommunications Union
JLOS	Justice, Law and Order Sector
MDAs	Ministries, Departments and Agencies
MoES	Ministry of Education and Sport
MoICT & NG	Ministry of ICT and National Guidance
MoJCA	Ministry of Justice & Constitutional Affairs
MoPS	Ministry of Public Service
MSME	Micro, Small and Medium Enterprises
NCII	National Critical Information Infrastructure
NCDC	National Curriculum Development Centre
NCS	National Cybersecurity Strategy 2016 (draft)
NIISP	National ICT Initiatives Support Program
NISAG	National Information Security Advisory Group
NISF	National Information Security Framework
NISS	National Information Security Strategy
NITA-U	National Information Technology Authority - Uganda
ODPP	Office of the Director of Public Prosecutions
PKI	Public Key Infrastructure
PPP	Public-Private Partnerships
R&D	Research and Development
SDG	Sustainable Development Goals
UCC	Uganda Communications Commission
UG.CERT	Computer Emergency Response Team of the communication sector
UGX	Uganda Shilling
UN	United Nations
UNBS	Ugandan National Bureau of Standards
UPF	Uganda Police Force
WB	World Bank

FOREWORD

This century is witnessing a fundamental change in our way of life with the advent of new epidemics such as covid19 coinciding with the Fourth Industrial Revolution where advances in Information and communications Technology (ICT) have blurred the boundaries between the physical, digital and biological worlds. ICT has experiencedincreased uptake in the country and has the potential to provide rapid social economic transformation by enabling efficient production and improved service delivery. These technologies however continue to be exploited by malevolent users with the phenomenon becoming intrinsically linked to organised crime on the internet and internal practices that exploit weakness within information systems.

National Development, economic growth and provision of basic services have hence become inextricably linked to the existence of secure and sound ICT systems and infrastructure. As a matter of fact, ICT systems have become a key element in the delivery of polices at the international level such as the Sustainable Development Goals (SDGS) and the Uganda Vision 2040 at the National level, particularly with regard to addressing the universal need for development.

The National Cyber security Strategy sets the direction for secure management of the country's information and communications technology resources with the view to ensure sound operation and safeguard them from information security threats. The Government is aware that the path to achieving effective protection of ICT resources requires focused and strategic interventions across Government and the Private Sector.

The strategic interventions to be undertaken will encompass the following key areas among others;

i) Building of a Safe and trusted digital economy;
ii) Enhancement of Threat preparedness and response;
iii) Development of a Robust cybersecurity ecosystem;
iv) Capacity building on Cyber skills;
v) International cooperation and building of linkages with the Global cyber security community;
vi) Provision of an enabling governance framework for cybersecurity in Uganda;

Government is committed to securing the use of ICT systems in the country to ensure the provision of an enabling environment comprised of efficiencies in production and service delivery that will spur economic development and prosperity for all.

I thank all stakeholders that have made contributions towards development of this strategy and appeal to all implementation agencies to dedicatedly undertake their respective interventions and so ensure the sector contributes effectively to the social economic transformation of our great nation.

FOR GOD AND MY COUNTRY

Hon. Dr. Chris Baryomunsi, MP
Minister for ICT & National Guidance

EXECUTIVE SUMMARY

Over the years, the Government of Uganda has placed the required enabling environment to facilitate the growth of the information and communication technologies (ICT) sector. Uganda has invested in a national fibre-optic back- bone to promote social and economic development by availing cost effective, reliable and high-speed connectivity to businesses and citizens. In the last ten years, Uganda's ICT sector has grown at an exponential rate, owing largely to a favourable policy and legal climate that has resulted in increased investment, expansion of ICT infrastructure, innovation, and expansion of ICT products and services. The potential for the total transformation of the economy and the attendant social impact is best demonstrated by the pervasive expansion and use of mobile money services in Uganda. According to the statistics of the Bank of Uganda the mobile money transactions facilitated via telecommu- nication company platforms more than doubled in value from 9$ billion in 2015 to US 26$ billion in 2020. The recent National Development Plan III for 25/2024 – 21/2020 stipulates the Country's medium term strategic direction, development priorities and implemen- tation strategies in line with the Uganda Vision 2040, and sets the digital transformation, i.e. the usage of ICT services for social and economic development, as one of the 18 core programs of the strategy.

At the same time, peace, security and defence are prerequisites for a sustainable socio-economic transformation, democracy and national unity. The growth in the ICT infrastructure, Internet usage and online access have opened new opportunities for the country, however, with the increase in use of e-services, the need for cybersecurity protection is key in order to avoid cyber fraud and maintain trust in the use of these services. Information security also serves broader national security goals by protecting critical national sectors and information infrastructure.

Security in cyberspace is especially important to realize the strategic visions of Uganda. This Cybersecurity Strategy 2022 provides development paths, policy and technical recommenda- tions to achieve Uganda's Vision 2040 aiming to transform Uganda into a competitive upper middle income country. Uganda has taken important steps to put in place and implement in practice the necessary policy, legal and regulatory frameworks in order to take advantage of the growing digital economy, but also to protect its critical national infrastructure and citizens, by ensuring a safe and secure space that will help the society to have trust and confi- dence in the digital economy.

The Cybersecurity Strategy 2022 is a strategic planning tool that reflects Uganda's plans to achieve the objectives of modern economies. The strategy contributes to existing policies that seek to implement Uganda's socio-economic development from cybersecurity perspective and aspires to support building a digital environment that citizens and businesses can trust.

The Strategy document is structured in four main chapters. First, the vision, mission and goals for Uganda are set for the next years in the cybersecurity domain. Next, the Strategy describes the context of today's trends in digital development and Uganda's strategic advances. It further introduces cyber threats and trends in cybercrime, and the national capacities to address these. The essence of the Cybersecurity Strategy 2022 is in Chapter 3, which describes the main principles, strategic direction, pillars and targets in six areas. The last Chapter covers the implementation mechanism as well as the monitoring and evaluation of the strategy. The Strategy was developed through a consultative process led by the Ministry of ICT and National Guidance.

1. VISION AND GOALS

1.1. Vision and mission

Vision: Uganda is a Digitally Empowered Society and Knowledge Economy.

Mission: To create a cybersafe and protected Uganda by ensuring a secure and resilient cyberspace that supports the adoption and innovation of ICT in all sectors for the socio-economic stability and development of Uganda.

1.2. Goals

Digitalization is an important process that supports Uganda's economic development, national welfare, and prosperity. Our goal is to have ICTs incorporated into every aspect of the everyday lives of people, organisations, businesses and government. The national cybersecurity system to be established by this Strategy aims to support the fostering of a safe and trusted digital economy of Uganda, to ensure the safety of e-services, and to reduce cybercrime. The strategy sets strategic goals in 6 areas.

Cybersafe and protected Uganda

Strategic goals	Safe and trusted digital economy	Threat preparedness and response	Robust cyber security ecosystem
Keywords	Trusted e-services, PKI and strong eID, Skilled MSMEs	Risk management, Preparedness, Incident response	Protection of the National Critical Information Infrastructure, Public-private partnership, Supply chain risks
	Cyber skilled Uganda	Active and reliable partner of the international community	Provide an enabling governance framework
	Cybersecurity curricula, Improved expertise, Awareness raising, R&D	Bi- and multilateral cooperation, Regional cooperation, Capacity building	Coordinated governance, Updated legislation

Strategic goals

Keywords

Following the whole-of-nation principle

The protection of Uganda and its citizens in cyberspace is a shared responsibility everyone has a role to play. The COVID crisis has shown the importance of secure online connectivity as it is forcing anything which can be digitized, to digitize and many organisations have had to embrace remote working. The whole-of-nation principle calls for citizens, private sector companies, and government agencies to work hand-in-hand to seize the various possibilities of digital technology while managing cyber risks.

The Government of Uganda is putting in place the necessary infrastructure and policies to build capabilities, and to create a conducive ecosystem for the Digitally Empowered Society and Knowledge Economy of Uganda as set in the Digital Uganda Vision. In addition, the Government is conducive ecosystem to foster Uganda's cybersecurity by developing and enforcing policies and guidelines. However, both companies and community as important stakeholders shall do their part and follow national cybersecurity guidelines and policies set by the Government.

2. CURRENT SITUATION,NATIONAL CAPACITY ASSESSMENT AND TRENDS

E-Services and the enwidening use of ICT are the lifeblood of the digital economy globally. Over the last two decades, the number of e-Services globally has accelerated exponentially, helping to connect industry, facilitate trade, and drive international investment.E-Services have also impacted environmental and social practices and transformed the delivery of government services.

Uganda Vision 2040 aims at "a transformed Ugandan society from a peasant to a modern and prosperous country within 30 years". As a developing country, Uganda has a unique opportunity to boost economy, public administration, education, and healthcare with dig- italisation. Without outdated legacy systems it is possible to focus on new opportunities in technology and e-services. Digital transformation also positions Uganda among regional and global leaders in the field of digital agile governance by focusing on effective service delivery, citizen engagement and the digital economy. This will reduce the cost of gove nance and reduce corruption while increasing national productivity.

The potential for the total transformation of the economy and the attendant social impact is best demonstrated by the pervasive expansion and use of mobile money services in Uganda. Mobile money transactions facilitated via telecommunication company platforms more than doubled in value from 9$ billion in 2015 to US$ 20 billion in 2019, according to the Bank of Uganda. Further design and implementation of specific sector-wide digitalization projects can assist faster and more profound digital transformation.

Transformation of Uganda to modern society will rely on a modern education system but also on high awareness and safe behavior while using ICTs. Uganda focuses on building a digitally enabled society that is agile and able to adapt to emerging technologies and trends. It also looks at promotion of digital literacy and ICT professional development for the current and future industry needs.

Cybersecurity is the a cross-cutting theme to support the digital economy and transformation. Therefore, it is important to develop also a robust and solid Cybersecurity Strategy that establishes measures to ensure security of digitalisation process and help to protect Uganda and its citizens in cyberspace. The strategic tasks described in the Cybersecurity Strategy will give assurance that digital services are and will remain safe, secure, protected, and trusted.

2.1. Alignment with other strategies

Uganda has established a solid set of strategic perspectives, with the wider aspiration to support Uganda's economic competitiveness and growth enabled by ICT. A series of policies, strategies, and legislation provide the road map guiding the country to becoming an information society and digital economy and set the guiding principles and direction for the Cybersecurity Strategy 2022.

Uganda Vision 2040 emphasizes the importance of digital transformation in Ugandan society and underscores the need for Uganda to reorient itself to make ICT as the main driver of economic growth. **Digital Uganda Vision** of the Ministry of ICT and National Guidance provides an overarching framework that responds to the national Vision 2040 by providing a unified ICT policy direction and strategic framework to show how ICT can empower Ugandan citizens and achieve the goals of universal inclusion, sustainable development, economic progress and poverty eradication through digital innovation. Digital Uganda Vision acknowledges that the ICT potential by different stakeholders is very much premised on the ability to ensure security of information, privacy and protection of personal data. Therefore, the Vision provides strategic inventions to build a trusted digital ecosystem in Uganda.

The **4th Industrial Revolutions Strategy's** (4IR) vision is to transform Uganda to a continental 4IR hub by 2040 and accelerate Uganda's development into an innovative, productive and competitive society using 4IR technologies. One of the strategic objectives is to support national security in the digital world. In near future, businesses are becoming deeply reliant on technologies such as Internet of Things, Artificial Intelligence, Big Data, and cloud computing that are all dependant on connectivity, which inadvertently would open up even more avenue for potentials risks and threats to security. However, the investment into the development of new technologies enables timely detection and response to a cyber incident.

Given the immense advantages of connecting the population to the internet and to mobile networks, both universal broadband access and complete mobile coverage nationally are national priority in terms of infrastructure. **Uganda Broadband Policy 2020** recognizes the broadband infrastructure as a public utility (like water, transport and energy) and sets the target to provide connectivity for all, improve its affordability and licensing conditions.

At the same time, peace, security and defence are prerequisites for a sustainable socio- economic transformation, democracy and national unity as stated in the Uganda Vision 2040. Security in cyberspace is especially important to realize the goals set in the Digital Uganda Vision. Protection of the country's sovereignty is now the next frontier and Uganda needs the enhanced the capabilities and resources, both human and technological, to build adequate and credible defence capacity to address external threats and maintain internal security.

Third National Development Plan 2020/21–2024/25 acknowledges that cyberspace is now a medium for disinformation among competing commercial interests, ideological adversaries, governments, and extremists, and it is a battleground between cybercriminals and law enforcement.

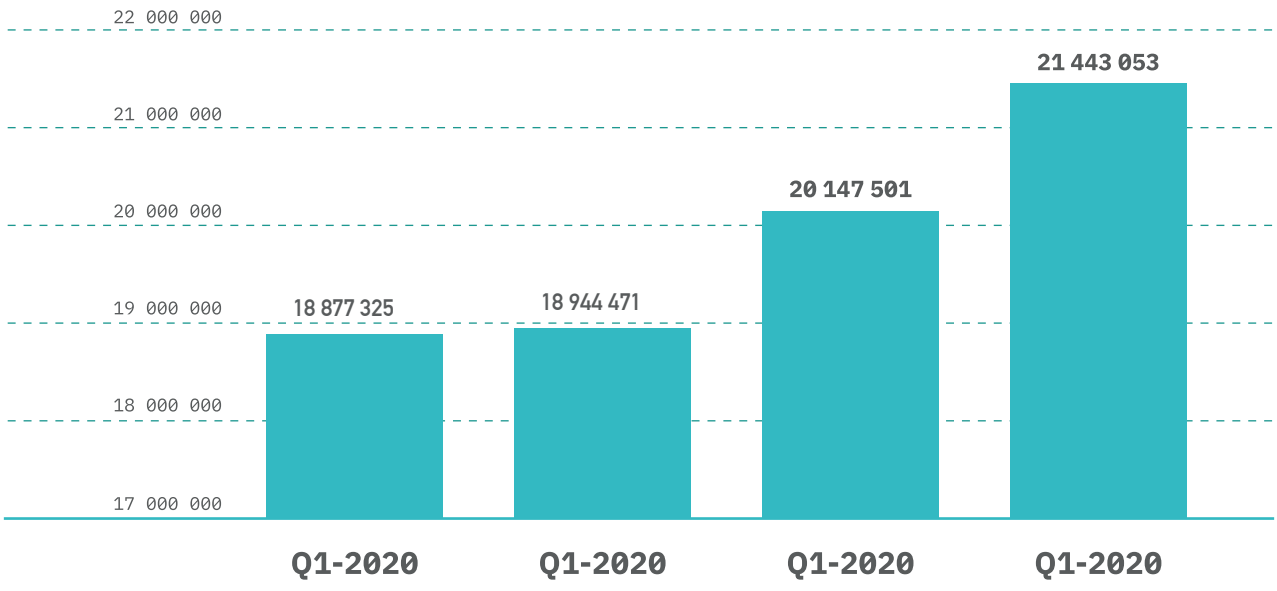
The Plan emphasizes Uganda's need to significantly invest in building the competencies of communication structures to be able to anticipate, avert and stop disrupting attempts of government or commercial operations and minimize the spread of misinformation. Government is willing to react and enact regulation of cyberspace, increase resources for cyber-defence and protect the critical infrastructure (e.g. power grids) from cyber threats.

Uganda's preparation of its National Development Plan coincided with the endorsement of the **UN2030 Agenda for Sustainable Development** in 2015. Consequently, Uganda was among the world's first to begin alignment of the Sustainable Development Goals (SDGs) with its national planning frameworks. The aspiration of the Agenda is to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation by 2030. Similarly, the **Agenda 2063 of African Union** aspires is to put in place neces- sary infrastructure to support Africa's accelerated integration and growth, technological transformation, trade and development.
All these goals can be linked to the main strategic documents of Uganda.

2.2. Digital Transformation of Economy

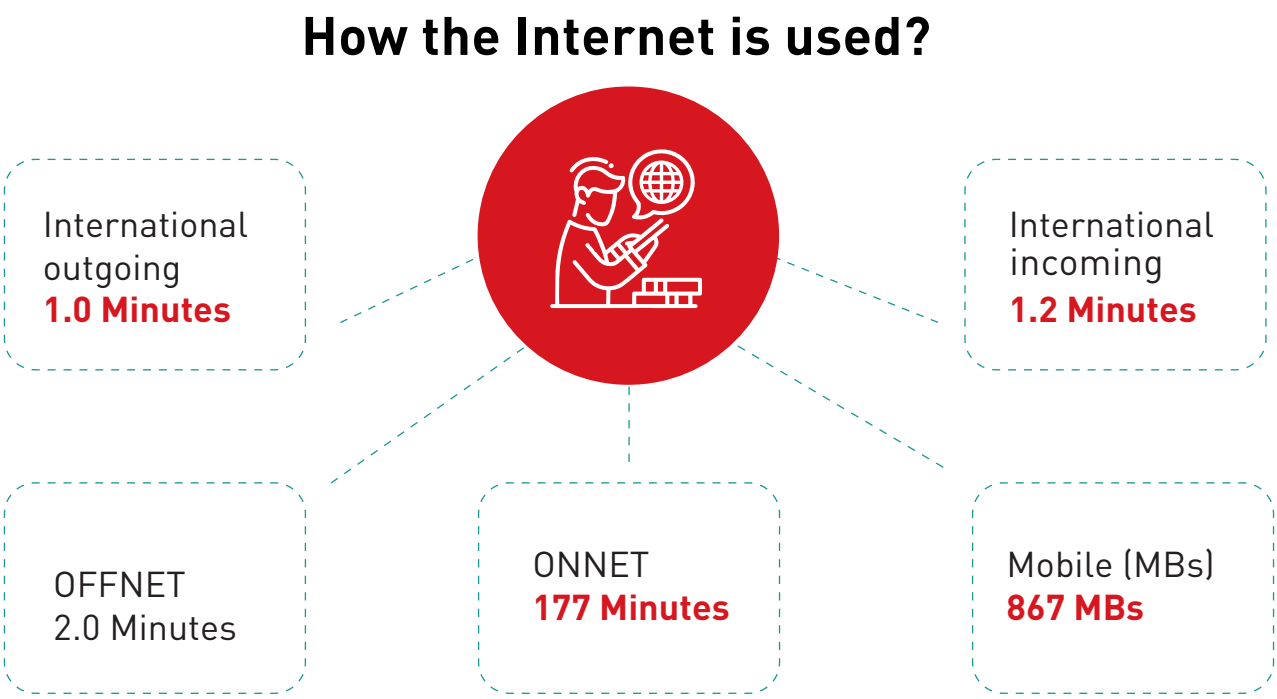
In the end of 30.8 ,2020 million devices were connected to the network in Uganda. These include mobile handsets, laptops, tablets and other IOT terminals. The growth is significant during the last 12 months 3.7 million new devices were connected to the network. Based on the UCC Market Performance Report 2020, in December 2020 the number of active internet subscriptions had grown to 21.4 million which means more than 1 active connection for every 2 Ugandans. According to the ITU Digital Development Dashboard 24 2020 % of Uganda's population is using the Internet (data from 2017) thus positioning as average in the African region, with significant potential for growth.

Figure 1. Mobile and fixed Internet subscriptions in 2020 (Source: Bank of Uganda, 2020).



However, broadband access in Uganda is largely mobile and rate of fixed broadband pen- etration is still very low (0.1 % of all Internet subscriptions in the 4th quarter of 2020 are fixed). The low fixed broadband access implies that there is little progress in promoting broadband access to anchor institutions like schools, libraries, health centers, and Local Government offices and that a critical mass of institutions and businesses are not using broadband services to be competitive.

Figure 2. How the Internet is used? Monthly user traffic profile in 4th quarter of 2020 (Source: Bank of Uganda,2020 (2020).

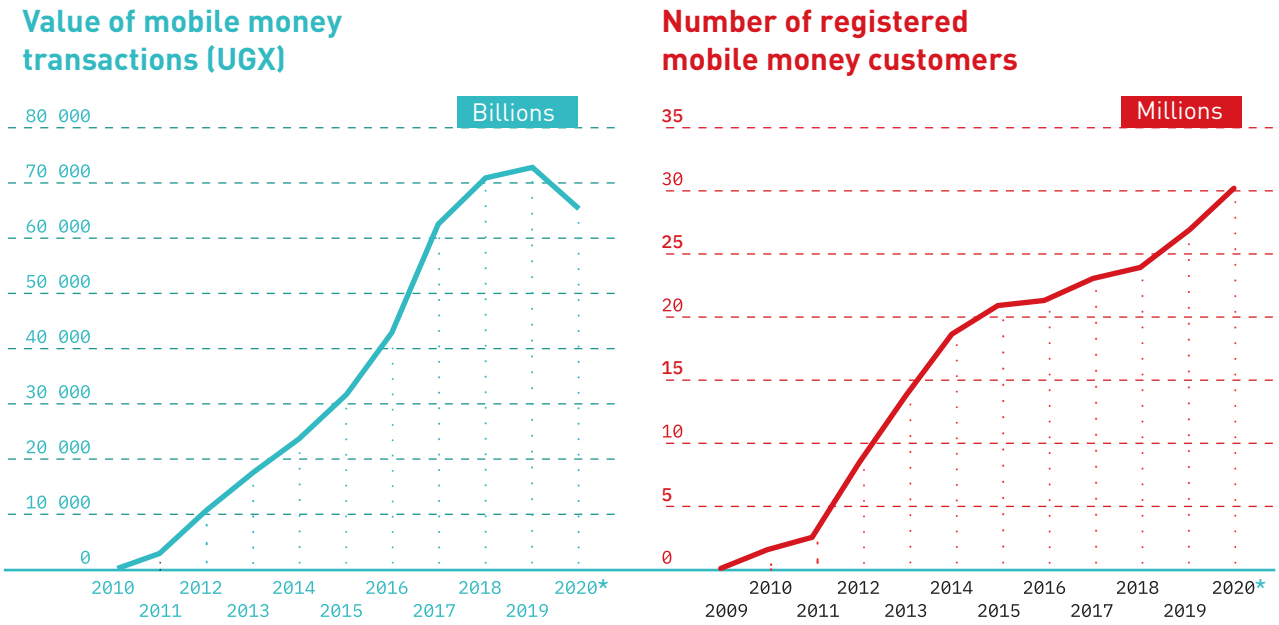


In recent years, and in particular during the global pandemic crisis, Uganda has witnessed an increase in malware distribution, business email compromises, the spread of fake news and mobile money network fraud. In early October 2020, Uganda's telecoms and banking sectors were plunged into crisis due to a major hack that compromised the country's mobile money network. At least 3.2$ million is estimated to have been stolen in that incident, in which hackers used around 2,000 mobile SIM cards to gain access to the mobile money payment system.

By the end of 2020, total active mobile money accounts stood at 22.5 million of the 28 million registered accounts. The trend in the mobile money industry and the growth in number of mobile money accepting businesses has been upward for the year 2020. The number of active mobile agents has grown to 235,790 and the number of mobile money transactions during the last quarter of 2020 for the first time ever crossed the 1 billion transactions mark.

In many African countries however, Uganda included, mobile data baskets are still out of reach for a large part of the population, costing more than 10 per cent of Gross National Income per capita, in situations where incomes are already limited. ITU analysed the digital trends in Africa and in terms of affordability of fixed services, Africa is the region with the highest fixed broadband basket prices and Uganda is no exception.

Figure 3.
The use of mobile money up to September 2020 (Source: Bank of Uganda, 2020).



* Only upto September 2020

The private sector in Uganda is dominated by about 1.1 million micro, small and medi- um enterprises (MSMEs) all together employing approximately 2.5 million people. The Uganda Vision 2040 aspires directly investing in strategic areas to stimulate the economy and facilitate private sector growth and targets increasing the growth of MSMEs to drive industrialization. National Development Plan recognizes the need to support the private sector, particularly local MSMEs, to develop capacity to drive the industrialization effort, increase exports, create jobs and increase local content. In the strategic ICT sector, SMEs can be supported through the system of incubation centres to develop their digital and financial literacy, and through supportive research and innovation facilities established and accessible to MSMEs.

The 2018 After Access Survey shows that Internet use, mobile phone penetration, and the Internet use divisions between genders as well as urban and rural dwellers are correlated with Gross National Income (GNI) per capita. Uganda is classified as one of the least devel- oped countries – a list of developing countries that, according to the UN, possess the lowest indicators of socioeconomic development and the lowest Human Development Index ratings among all countries in the world. The lack of electricity and underdeveloped ICT infrastructure are the primary causes of discrepancies in urban–rural Internet use and mobile phone penetration rates in Uganda. Uganda has a considerable urban–rural gap in Internet use of 70 percent, where only nine percent of Ugandans living in rural areas have access to the Internet and about a third (30%) of urban area dwellers using it[1].

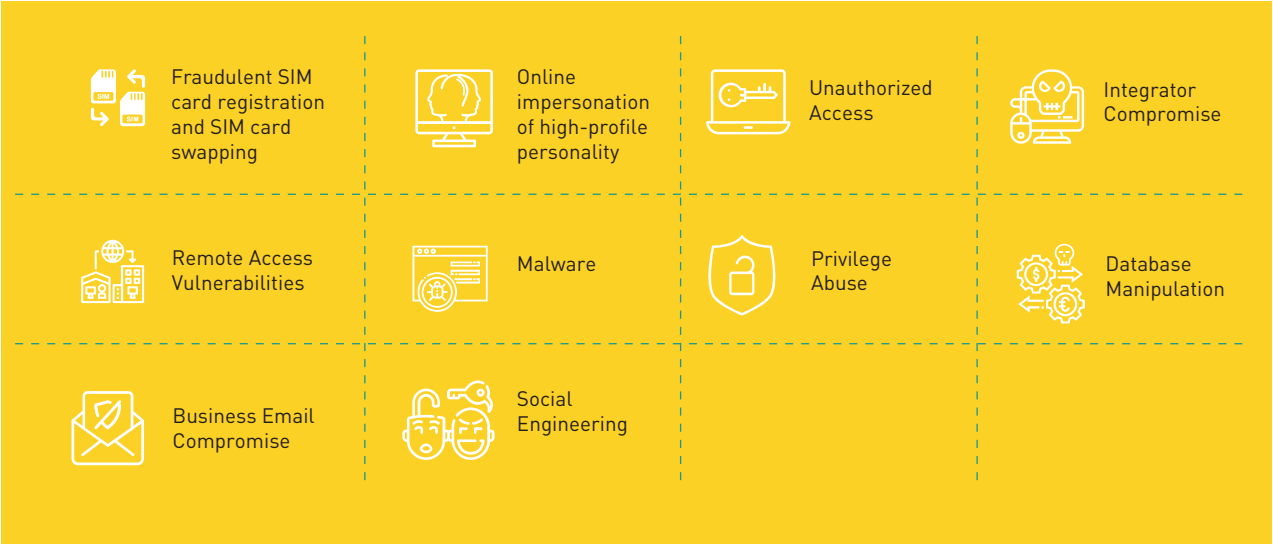
Several studies demonstrate that broadband penetration and broadband quality are im- portant factors for economic growth. According to a World Bank study, it is estimated that for every 10% increase in broadband penetration in low and middle income countries result in a commensurate increase of 1.38% of the GDP [6]. Studies also reveal the economic impact of broadband deployment directly through jobs created by deploying broadband infrastructure, and indirectly as a result of 'spillover' externalities, such as increased productivity and new products and services i.e., through accelerated innovation.

1 Gillwald. A, Mothobi, O., "After Access 2018.
A Demand-side View of Mobile Internet from 10 African countries", Research ICT in Africa,2019.

2.3. Cyber Crime

Cybersecurity continues to be a challenge in Uganda and the share of cyber (computer) crimes in total economic crimes is on the rise. In 2020 the cybercrime report of the Uganda Police acknowledges the relative increase in cases of cybercrimes related cases and they led to a loss of UGX 15,949,236,000 in 2020, of which less than 0.05% (UGX 7,720,000) was recovered. Two major categories of cybercrimes were electronic fraud and obtaining money by false pretense. In addition to economic crimes, cybersecurity threats pose a serious risk to the integrity of the e-government system and internet in Uganda generally[2].

Figure 4.
Major categories of cybercrimes (Serianu, Africa Cybersecurity Report. Uganda, 2019/2022).



The Uganda Police Force has digital forensics capacity and a cyber-crime unit. The cybercrime unit helps the Police to participate and get knowledge on current trends on cyber security. Police in collaboration with the Ministry of ICT and National Guidance, National Information Technology Authority Uganda (NITA-U) and the Uganda Communications Commission (UCC) have published several cybercrime awareness materials and initiated thematic campaigns. Cybercrime is reported to have had a 300% fold growth in the year 2020[3], thus the need for capacity building is urgent to cope with the increasing number of cybercrimes.

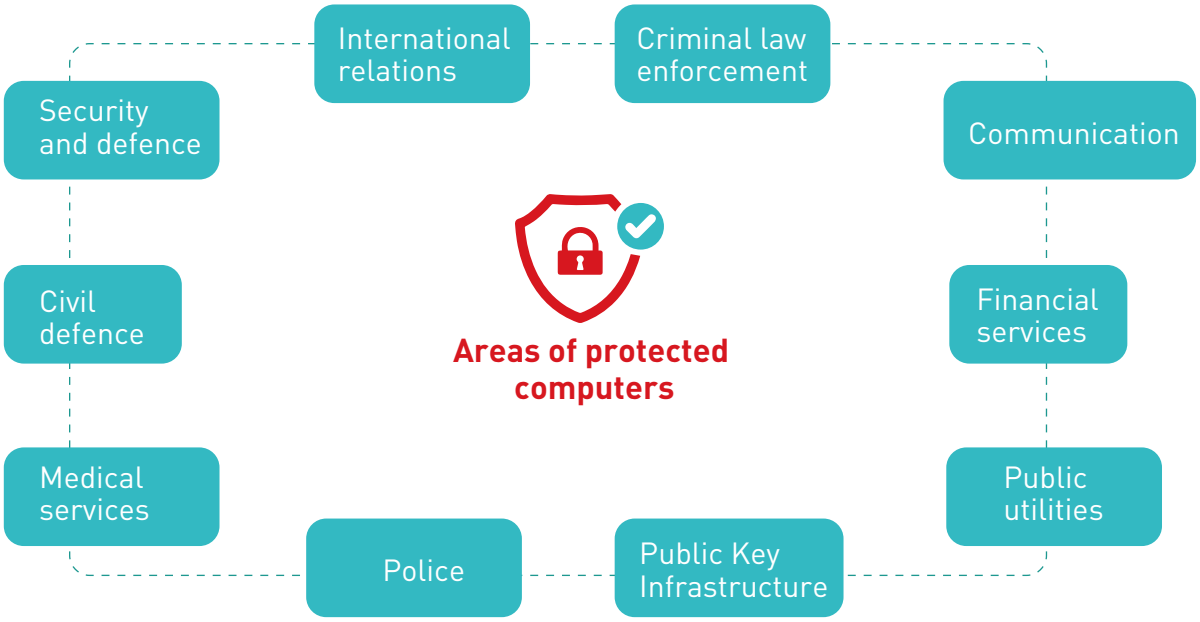
2 Uganda Police Force, Annual Crime Report 2020.
3 SERIANU, Africa Cybersecurity Report. Uganda, 2020/2019.

2.4. Protection of critical infrastructure

In 2011, the Government of Uganda through the Ministry of ICT developed the National Information Security Strategy (NISS) supporting sub-sector policies and frameworks within the ICT sector to secure critical national infrastructure and information resources. The NISS recognizes the importance of the identification of critical infrastructure that are critical for the functioning of the society as a whole.

The Computer Misuse Act 2011 provides guidance on sectors that are currently recognized as Critical National Infrastructure sectors in Uganda. According to the Act, a "protected computer" is a computer, program or data used directly in connection with or necessary for the security, defence or international relations of Uganda; law enforcement; the provision of services directly related to communications infrastructure, banking and financial services, public utilities; public key infrastructure and public safety. The National Information Security Policy and Framework (NISF) with its compulsory security measures applies to all organisations that operate protected computers.

Figure 5.
Areas of protected computers according to the Computer Misuse Act 2011.



The establishment of security baseline for protected computers, programs or data in sectors specified in NISF and Computer Misuse Act (2011) has been the tool to address the national critical information infrastructure (NCII) protection in Uganda. However, in the current regulative framework does not provide for obligations for cyber-incident reporting, which remains ad-hoc activity and thereby exacerbates the potential impact of incidents.

The latest development in the area is the Strategic Plan on the protection of National Critical Information Infrastructure approved by the Ministry of ICT and National Guidance as well as NITA-U in 2021. The document describes critical infrastructure sectors, the CNII operators as well as their role.

2.5. Digital awareness

With the rapid growth of internet connectivity on the African continent, many Ugandans are getting access and connecting to the internet for the first time, while often lacking knowledge on how to protect themselves online. Low levels of ICT literacy would make it difficult to launch such campaigns, which the Global Cybersecurity Capacity Centre found to be almost non-existent in the African countries it surveyed. In 2017, 90% of African businesses were operating below the cybersecurity 'poverty line' – unprepared for cyber threats and an easy prey to cybercriminals[4].

The Government of Uganda has realized that cybersecurity awareness is crucial and considerable awareness raising efforts, coupled with increasing availability, access and affordability have been undertaken. These efforts include concerted ICT security aware- ness campaigns led by the MoICT & NG, NITA-U and UCC. For example, a review of NITA statistics report 2019 indicates 'Sensitization activities to enhance cyber legal awareness' have been conducted over the years. In July 2021, Government through the National In- formation Technology Authority - Uganda embarked on a digital awareness campaign on cybersecurity with funding from the Regional Communications Infrastructure Program. The development and continuous implementation of cybersecurity awareness initiatives, focusing on disseminating information about cybersecurity risks and threats, as well as about best practices for countering them, should be continued and enhanced.

In addition, there is a need for a structured training and certification program/framework for cybersecurity related careers in Uganda. Education on ICT and security issues is not offered as part of the curriculum in all levels of education, and there is limited budgetary allocation for research and development in this field. Gaps in information security in the country can be close best by integrating security into the education systems and making skill building easier and attainable.

2.6. Uganda's Performance on Global Indices

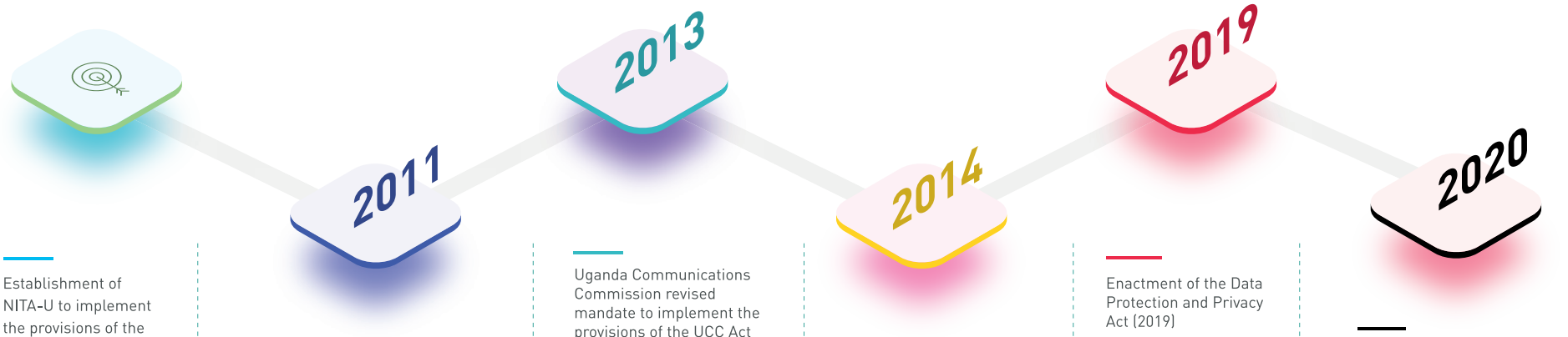
Uganda has set the goal to improve rankings in the various global competitiveness indices. According to World Bank annual ratings Uganda is ranked 127 among 190 economies in the ease of doing business in 2018, a position it maintained in the following year (2019).

Uganda ranked 152 out of 176 countries in the **International Telecommunications Union's IDI** (2017); 121 out of 139 countries in the **Network Readiness Index**; and 64 out of 75 countries in the latest Economist Intelligence Unit **Inclusive Internet Index** (3i). Behind these rankings is the poor information infrastructure and low levels of Internet penetration in the country compared to others. **In terms** of **Internet freedom**, Uganda is considered as partly free and Internet penetration rates continue to improve despite a daily tax on social media use that limits access to communication platforms. In the **E-Government Development Index** (EGDI), which presents the state of E-Government Development of the United Nations Member States, Uganda ranked 137 out of 193 countries in 2020.

In the ITU Global Cybersecurity Index; in the African region Uganda ranks as 9th in 2020 (2018 7th), globally 70th (2018 65th). According to the index, the Uganda's relative strength is in the implementation of legal measures but there is room for potential growth in the Cooperative Measures category (national, regional, and international cooperation), implementation of the Data Protection and Privacy Act and also in capacity building. In the **National Cybersecurity Index** of the e-Governance Academy, Uganda holds 56th position globally and 3rd in African region.

4 EU Institute for Security Studies, 2021. Digital Dialogue. Africa as a Cyber Player.

Current Cybersecurity Strategy 2022 builds on the following milestones:



Establishment of NITA-U to implement the provisions of the NITA-U Act.

2011

Several laws were promulgated to guarantee a safe online environment for users and citizens, with a number of texts developed, namely the Computer Misuse Act (2011), the Electronic Signatures Act (2011) and the Electronic Transactions Act (2011).

Adoption of the National Information Security Strategy (NISS)

2013

Uganda Communications Commission revised mandate to implement the provisions of the UCC Act 2013

2013-2014
Establishment of Computer Emergency Response Teams: Uganda National CERT.UG/CC and Communications Sector UG-CERT

2014

Publishment of the draft of the National Information Security Policy and Framework (NISF)

Establishment of the National Information Security Advisory Group (NISAG) as forum for providing guidance to Uganda's critical Infrastructure operators

2019

Enactment of the Data Protection and Privacy Act (2019)

2020

Publishment of the draft of the Digital Uganda Vision

3. STRATEGIC TASKS
3.1. Safe and trusted digital economy

- Develop and implement digital identity to facilitate the utilization of e-services
- Prioritize support for MSMEs

The real potential for economic growth and large-scale job creation lies in spreading digital innovations from lead firms to the rest of the economy. The role of governments is to create an environment that enables the many private sector actors to benefit from digitalization. Studies demonstrate that broadband penetration and broadband quality are important factors for economic growth. They also reveal the economic impact of broadband deployment directly through jobs created by deploying broadband infrastructure, and indirectly by increased productivity and the creation of new products and services. According to a World Bank study, it is estimated that for every 10% increase in broadband penetration in low- and middle-income countries, there is a com- mensurate increase of 1.38% of the GDP[5].

3.1.1 Implement PKI and e-Signature

Government will make effort to create an online environment that is safe and trusted by society and businesses. The vision is a user-friendly digital ecosystem where the security of personal and sensitive data and information is assured, and users' rights are protected.

To improve the trust and confidence towards digital transactions and e-services, the Government will **enforce the adoption and implementation of digital standards, laws and regulations that ensure security of online transactions** Uganda has taken steps towards a safer service environment. The Electronic Signature Act 2011 together with relevant regulations provide a framework for the provisions and use of electronic signatures. The Act regulates the use of advanced electronic signatures, digital signatures and the use of third-party certification systems, such as a public key infrastructure (PKI), for the purposes of securing information conveyed over the internet and authenticating or certifying electronic signatures. Government of Uganda through NITA-U is implementing the UgPass pilot project, a new digital authentication and electronic signatures' solution for Uganda which will activate the use of PKI services.

5 Kim, Y., Kelly, T., and Raja, S., "Building broadband: Strategies and policies for the developing world.," The World Bank, 2010

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

Uganda will take advantage of rapid advances in digital technology to establish national digital ID platforms or systems that serve the whole nation, including enterprises. Digital ID and signature are vital components of the modern economy, without which digital transformation will be impossible.

3.1.2 Increased focus on enterprises

African economic growth has been steady for 25 years, but the continent has not fully enjoyed the benefits of digitalisation for economic and social progress. Also, policy makers are becoming more aware of the need to secure the digital future, as cybersecurity became part of the African Union Agenda 2063. Business operations have shifted further online during the COVID-19 pandemic, placing increased demands on private sector cybersecurity practices. MSMEs are often the most common size of business within a country and make up a significant part of national economy as 90% of businesses are MSMEs, 50% of employment stems from MSMEs, and formal MSMEs contribute up to 40% of Gross Domestic Product in emerging economies. Thus, Uganda has to nurture entrepreneurship and innovation.

MSMEs are also often least able to tackle cybersecurity. This puts MSMEs in need of cybersecurity awareness activities and accessible cybersecurity tools. The Government will provide its support and run **dedicated programs for MSMEs** to enhance the awareness how to safely conduct business in today's networked environment. Uganda through the **Ministry of Trade, Industry and Cooperatives** and by involving the associations of MSMEs (like the Federation of Small and Medium Enterprises-Uganda, the Uganda Small Scale Industries Association etc) will develop a collaborative platform that will help micro, small and medium size enterprises to protect their organizations against the most common cyberattacks. Governmental cybersecurity **web portal** will provide guidelines and awareness-raising materials and initiatives focused on MSMEs.

The compromise of personal data can damage the legitimate rights and interests of cause adverse disruptions to the affected individuals and businesses. With increasing amounts of data migrating to computer systems and electronic devices, there is a need to secure these systems and safeguard individuals' data against theft and misuse. At the same time, organisations can leverage good personal data management to gain a better understanding of their customers, increase business efficiency and effectiveness, and boost customer confidence.

Uganda through the **Personal Data Protection Office** will intensify the work with private organizations to **embrace data protection** as part of their corporate culture and take reasonable steps to manage and secure the personal information that they hold. Through industry briefings, online training resources, and advisory guidelines, MSMEs will be equipped with information on the requirements of the Personal Data Protection Act and good data management practices.

The Government will take the lead in introducing a cybersecurity scheme to support the local cybersecurity industry and continuously expand the government's budget for cybersecurity. Thereby, the Government supports MSMEs to grow into competitive companies.

To strengthen the market opportunities, GoU will facilitate access to new market segments for domestic cybersecurity companies and promote locally made solutions.

3.1.3 Action Areas

By fostering safe and trusted digital economy, the Government of Uganda (GoU) will:

Implement digital identity to facilitate the utilization of e-services

The GoU will pilot the UgPass to implement a whole-of-nation PKI and deploy the essential enabling building blocks for modern and safe e-services. The standards for electronic signatures will be updated and specified. The GoU will continue to scale the usage of PKI within government IT enabled services and applications as well provide this as shareable infrastructure for private sector.

Prioritize support for MSMEs

GoU will provide our support by providing cybersecurity guidelines and stan- dards for voluntary compliance and dedicated capacity building programs for MSMEs to enhance the awareness on how safely conduct business in today's networked environment. As part of the program, GoU will work with private organizations to embrace cybersecurity and data protection as part of their corporate culture.

Expand cybersecurity investments

GoU will support the local cybersecurity industry to play a key role in im- proving the nation's cybersecurity level through the continuously expansion of the government's budget for cybersecurity. GoU will promote locally made solutions and facilitate access to new market segments for domestic cyberse- curity companies.

3.2. Threat preparedness and response

- Promote risk assessment practices based on central risk repository and publish Cyber Threat Landscape Report
- Develop central incident register and sectoral incident scenarios Strengthen national and sectoral CSIRTs Develop tools for information sharing
- Establish programs for a capacity building about risk management

3.2.1 Risk management

It is important to realize that cybersecurity incidents can never be completely prevented. The rapid development of technology and its accelerated spread also increases the potential for security incidents. Therefore, in addition to preventing incidents, the focus must also be on **cyber resilience** – i.e. on the **control and reduction of damage caused by incidents.** This requires two types of action: first, proactive measures aimed at preventing incidents, and second, reactive ones to control and reduce damage.

Figure 6.
Measures to achieve cyber resilience.

Continuous monitoring and analysis of information on security incidents both domestically and internationally makes the rapid identification of threats possible and the resolution of incidents more effective. Therefore, Uganda will put continuous effort to **identify and understand potential threats** (threat intelligence) **and the risks** associated with these threats (risk awareness). There is also a need for resources to **detect and cope with incidents** (incident management) and to plan activities and resources to **deal with the damage** caused by incidents (recovery). The existence of such measures will, on the one hand, increase the ability to prevent incidents by increasing overall security and, on the other hand, significantly reduce the adverse impact of incidents on society.

Global cyberattacks during recent years have caused a massive financial and reputational damage to states, governments, companies, and private citizens. To improve Uganda's resilience against such incidents, it is essential to **detect, analyze, understand, and mitigate cybersecurity risks.**

Cybersecurity risks involve three components:

1. **Threat.** Threat can be either technological, like malware, or geopolitical, like ad- versary nation state, crime, like an organized crime group, or even environmental like extreme weather conditions.

2. **Vulnerability.** Vulnerability is often described as a weakness of computer system which can be exploited. In the cyber ecosystem, vulnerability is more complex and the nature can either be technological, organizational, administrative or any other that might leave the ecosystem open.

3. **Consequence (impact).** Consequence can be assessed combining likelihood of the cyber incident with potential impact to the ecosystem or its components.

To mitigate cybersecurity risk and minimize the negative impact of cyber threats, Uganda will continue the **update of National Information Risk Register**, develop and regularly update **sector based risk scenarios** for incident management (for energy, communications, government sectors etc). Both national level and sector oriented cyber risk repositories improve understanding about current cybersecurity risks and allow to forecast and model trends. It is important that all considerable changes in technological risks should be included in risk. New risks, related to major shifts in technology like the use of artifi- cial intelligence, quantum computing etc. should also be considered. Similarly, risks that are related to growing use of existing technologies like cloud computing and IoT should also be considered in risk landscape.

The responsible regulatory bodies and NCII operators will update periodically the list of their critical services due to continually changing threat landscape.

Uganda will establish the mandatory incident reporting for NCII and government sector and aggregate a **national level incident register**, which is essential for understanding security situation and to plan, develop and implement appropriate security measures for different sectors.

For a successful and efficient risk management, Uganda will foster **inter-agency cooperation** in cybersecurity related matters, especially in information sharing, and will **establish special programs for a capacity building** for sectors that have less resources for cybersecurity such as MSMEs, healthcare institutions etc.

3.2.2 Preparedness and incident response

Today, organizations' ability to handle potential incidents is inevitable. Globally, 86,2% of companies are being compromised by at least one successful attack in 2021. Notably, this doesn't account for attempted attacks or those that went unreported.6 Even though when global investments to cybersecurity are enormous, due to the dynamics of cyberspace, fast growing number of threats and rapid digitalization, attack surface is increasing fast. Many of attacks and other incidents can be prevented by efficient threat intelligence, risk awareness and smart technological protection. However, since cyber incidents will con- tinue to take place, appropriate incident management and incident recovery framework shall be established for Uganda.

In order to efficiently respond to incidents, Uganda through the Uganda National CERT and Coordination Center will **define clear national working arrangements** for information exchange and incident response. ICT incidents tend to escalate very rapidly, thus the roles of the various organisations and agencies, cooperation arrangements and mechanisms for exchange of information must be defined and organised. Given the need for extensive cooperation with the private sector and with future **sector specific CSIRTs** (e.g., financial, energy, etc.), the Uganda National CERT and Coordination Center will guide sectoral CSIRTs to develop specific competences (such as security of industrial control systems) that are needed for incident management in the specific sectors.

The threat environment and criminal landscape is in constant change, which means that the Government needs new tools, approaches and creativity for incident managers at MDAs, NCII operators, police and law enforcement to stand a chance. Uganda will clarify common interests of various stakeholders and **create appropriate tools or methods for information sharing.** Communication and information sharing both within public sector and private sector and between public and private sector is a prerequisite for efficient response to incidents.

Sound incident and crisis management plans as well as general knowledge about threat landscape guarantees the preparedness for incidents. Uganda will **draft and establish national and sectoral incident resolution plans** as a part of national emergency planning and crises management.

Testing the rules and plans for information sharing and incident management guarantee their efficiency. **Uganda will regularly conduct cyber drills**. Drills will be organised both within teams and at the national level.

3.2.3 Action Areas

To be prepared for threats and guarantee a sustainable national level cyber risk management and response system, GoU will:

- **Promote risk assessment practices based on central risk repository and publish Cyber Threat Landscape Report**
  GoU will establish a mechanism for continuous gathering of threat intelli- gence and analysis at strategic and tactical level. That shall include collection and analysis of the information about strategic threat vectors such as geopolitical tensions, increasing cybercrime etc. as well as technical information of cyber-attacks, characteristics of malware etc. Common cyber risk assessment methodology will be established for MDAs and NCII operators. The National Information Risk Register will provide up-to-date information about current cybersecurity risks and allows to observe and predict trends.

- **Develop central incident register and sectoral incident scenarios**
  The GoU will establish mandatory incident reporting for NCII and the government sector, and develop clear guidelines for reporting. NITA-U through the Uganda National Computer Emergency Response Team and Coordina- tion Center will manage an aggregated national level incident register. The GoU will generate sector-based risk scenarios for incident management, and prepare national and sectoral incident resolution plans as a part of national emergency planning and crises management.

- **Strengthen national and sectoral CSIRTs**
  GoU will enhance capacity and capability for incident response especially heavily focusing on the proactive approach, increasing capacity building for the first level incident responders and home grown re-usable security moni- toring solutions for organisations.

- **Develop tools for information sharing**
  GoU will foster cooperation and communication between security, law enforcement and other government agencies and provide a framework for cyberthreat intelligence sharing. National emergency planning and crises management will be enhanced through the development of large-scale cyber incident management plans.

- **Establish programs for a capacity building about risk management**
  The GoU will establish capacity building programs for sectors that have less resources for cybersecurity, such as MSMEs or healthcare institutions.

3.3. Robust cybersecurity ecosystem

- Implement the strategic plan on the protection of NCII
- Raising awareness of supply chain risks
- Update of the minimal cybersecurity baseline for NCII operators
- Create effective governance and management structure for the protection of NCII

3.3.1 Strategic plan on the protection of National Critical Information Infrastructure

The complex and interconnected nature of cyberspace is such that ensuring **holistic cybersecurity** becomes a shared responsibility between the Government, private sector and other stakeholders as part of the country's national critical information infrastructure is run by the private sector. A robust national ecosystem guaranteeing cybersecurity requires the involvement of all key stakeholders, both state and non-state actors, and at national and international level based on collaboration.

This collaboration will be guided by the Ministry of ICT and National Guidance. Assets that are essential to the functioning and security of a society and economy of the country are Critical Infrastructure (CI). National Critical Information Infrastructure (NCII) are ICT systems that operate key functions of the critical infrastructure.

The protection of National Critical Information Infrastructure relies on regular and up-to-date risk assessments

The protection of NCII in Uganda is addressed from a **risk management perspective.** Regular risk assessments guide the identification of national critical infrastructure and services, whose disruption may have a serious impact on the security or economic well-being of citizens and harm Uganda's possibilities to benefit from digitalisation. A risk-based approach also enables to prioritize implementation of programs and policies designed to protect NCIIs.

Earlier strategic interventions, i.e. the 2011 NISS recognizes the prominence of protecting critical information infrastructure from disruption and the role of public-private partner- ships as one of the guiding principles of Uganda. The Computer Misuse Act addresses the offences in relation with protected computers in certain areas and economic sectors, how- ever, it does not organize transparently the principles and criteria for determining the NCII ecosystem, nor does it outline minimum cybersecurity baseline addressing NCII operators.

The establishment of a security baseline for protected computers, programs or data in sectors specified in NISF and Computer Misuse Act (2011) has been the current practice to address the critical information infrastructure protection in Uganda. In order to enhance the transparency and thereby boost trust between the private and the public sector, the Government will implement a **strategic plan on the protection of National Critical Information Infrastructure** containing a **list of critical sectors** to be considered as essential for the maintenance of critical societal and economic activities. The national level risk assessments provided by Ministry of ICT and National Guidance, NITA-U and NISAG will serve as a basis of reviewing the list and any future NCII updates.

3.3.2 Understand the risks and implement the security measures

The protection of NCII in various sectors exceeds the capabilities and mandate of any single Government agency. In Uganda, the National Information Security Advisory Group (NISAG), an inter-sectoral working group provides the platform for collaboration.

Considering the changing threat environment, the **update of the minimal cybersecurity baseline** for NCII operators is inevitable. However, this should be done cognizant of the maturity level of the country to avoid the adoption of requirements that are too stringent and not implementable in Uganda's current setting. The Ministry of ICT and NG, responsible regulators, NISAG and owners of critical information infrastructures will assess the cyberse- curity baseline and provide consistent updates to the baseline consistent with international standards and best practice.

NCII Governance model defines clear responsibilities of every stakeholder. Minimum cybersecurity baselines for NCII operators will be established with appropriate legislative mechanisms.

The baseline relies on the risk management approach and provides guidelines to NCII operators about the implementation of necessary security measures. It is required that **every operator** of critical services and infrastructure **implements security measures**. NCII operators prepare or update their **contingency plans** of critical ICT systems based on the national risk environment. Among others, the baseline will address incident response and vulnerability disclosure among other topics and the mandatory implemen- tation of the cybersecurity baseline by NCII operators that needs to be regularly audited.

Established formats for private-public partnership are essential for boosting trust amongst and between the industry and the government.

The Government continues working together with NCII operators to **promote understanding of cybersecurity risks**. The cooperation and exchange of information between government agencies and the private sector to identify cyber threats will ensure that the critical ICT systems are protected to a level that is commensurate with the risks faced, to ensure the operation and recovery of critical services and infrastructures. The National Information Security Advisory Group - NISAG provides a **cyber threat landscape assessment** based on the National Information Risk Register. Furthermore, **cyber incident reporting will be made mandatory** for all government authorities and NCII operators. The overview of incidents serves as basis for a comprehensive cyber threat landscape assessment. NCII operators are bound to report cyber incidents to their sectoral regulators, such is the current practice for the communication sector under Uganda Communications Commission. As referred in the previous chapter, NISAG's risk register helps to align cyber risk management with the country's national crisis/ contingency management plan. It can also help harness the necessary capabilities/ capacities, people, funding, and strategies to strengthen the overall cybersecurity posture of the Nation.

Guiding principles for NCIIs are the principles of personality and minimal adverse effects. Ensuring the security of a system is arranged by the service provider and in case of security incident, service provider will apply due care and measures to avoid the escalation and spread of the effect of the incident and will notify the supervisory authority.

Throughout the years, NISAG has been a platform for collaboration between NCII operators and the government sector. Through NISAG, they have shared the information on an adhoc basis. NISAG shall develop its procedures, document the NCII assets in the country and will promote a fluent information flow with oversight supervision from the MoICT & NG. Recognizing the critical and highly interdependent role of NCII operators in managing cybersecurity risks and responding to incidents, the Government will provide the **communication channels** and **cooperation mechanisms between public and private agencies**. For every critical sector, a National Regulatory Authority will be appointed, that serves as a sectoral contact point. The role of the contact points is to take lead on NCII protection within their sectors, to synthesize the information collected from NCII operators and con- tribute to the cyber threat landscape assessment at the national level coordinated by the Uganda National Computer Emergence Response Team and Coordination Center.

ICT service providers and NCII operators shall pay attention to risks that are related to **supply chain security**. Threat intelligence and respective risk assessments shall be monitored during the IT development stage and in the software and hardware tendering processes. The Government, though NITA-U, will develop the respective guidelines in collaboration with the Uganda National Bureau of Standards.

This Strategy aims to **create an effective governance and management** framework. Establishing sustainable partnerships among the Government and NCII operators re- quires that all participating stakeholders define a clear understanding of the goals of the partnership and the mutual security benefits that stem from dedicated and meaningful collaboration. Areas of cooperation include establishing effective coordinating structures and information-sharing processes and protocols, building trust through joint events and exercises that enhance cross-sectoral response, exchanging best practices for improving security, as well as improving international coordination.

- **Implement the strategic plan on the protection of National Critical Information Infrastructure**
  The strategic plan provides clear criteria on defining critical sectors and the roles and responsibilities of NCII operators, but also supervisory authorities to ensure the transparency and boosting trust amongst and between the government and private sector.

- **Raise awareness of supply chain security risks**
  GoU will increase the adoption of Security-by-Design practices and address cybersecurity issues upstream and along the supply chain. GoU will enhance the implementation of national cybersecurity standard for critical infrastruc- ture, including requirements for software and hardware that can be used in vital services. The Government will start the preparations for developing accreditation standards for hardware, software and IT services deployed in NCII.

- **Update of the minimal cybersecurity baseline for NCII operators**
  Based on international standards and best practice, GoU will enhance the implementation of security measures of NCII operators based on the regular risk assessments. To achieve the goal, the Government will set legal require- ments for minimum cybersecurity baseline of NCIIs. The standard includes the requirements for information sharing and incident reporting.

- **Create effective governance and management structure for the protection of NCII**
  The GoU through the Ministry of ICT and National Guidance will introduce legal provisions that give the relevant sector regulators the authority and resources to oversee compliance. This will assist in the efforts to implement the current strategy goals and achieve cross-sectoral agreements.

3.4. CyberSkilled Uganda

- Embed cybersecurity through all stages of education
- Improve expertise, skills and competencies
- Raising public cybersecurity awareness
- Enhance knowledge through research and development

End-users are often the **weakest link** in the cybersecurity chain. This is true when the users lack the training to take informed security decisions while carrying out digital activities. As people begin to become more connected, they need support to develop cyberse- curity capacities to better respond to threats. Securing the cyber domain through capacity building activities contributes to reducing issues such as cyber risks and the digital divide.

Promotion of the cybersecurity skills has been the main goals throughout the previous strategic interventions. However, a concerted effort by the Ugandan government to create online safety through skilled professionals and risk aware users demands an effort on continuous basis as the gap in the required skills set for cybersecurity still exists.

3.4.1 Embed cybersecurity through all stages of education

The review of the educational curricula is an ongoing task, and it shall meet current and future needs. To bridge the gap of institutional knowledge and shortage of skills Government of Uganda will promote and facilitate the development of cybersecurity educational programs. Inclusion of information security topics in the **national ICT related curricula** in all educational institutions across **primary, secondary and tertiary levels** is the goal. Curricula should be **interdisciplinary** and besides the technical knowledge also non-technical cybersecurity skills and topics, such as digital literacy, public policy and governance, economics, social sciences or international relations shall be covered.

The focus of Uganda is also on creating a skilled professional workforce based on local content and provide the required human resource pool. The Government will integrate **cybersecurity courses** in all computer science and IT programs in **higher education**, including computer security, forensics and processing electronic evidence, as a subject or field of expertise. Dedicated cybersecurity degrees and apprenticeships will be created, and additional resources for supporting the new degrees at the tertiary level will be applied. In addition, the curricula should foster awareness of and stimulate interest in cybersecurity career opportunities. To further the efforts in this space, the Government will consider various incentive schemes, such as scholarships and grants but also the estab- lishment of an accreditation mechanism for quality assurance of cybersecurity training programs in universities.

Given the multi-disciplinary nature of cybersecurity capacity building, universities, colleges, and other educational institutions should be encouraged to work across departments and with other academic partners to develop or update their programs. To achieve the goal, the cooperation and **collaboration between educational institutions** will be enhanced and a framework for delivering cybersecurity knowledge throughout the educa- tion system, especially in primary and secondary schools will be generated.

3.4.2 Improve expertise, skills and competencies

A qualified and highly skilled human resource base is pivotal for a successful information security strategy implementation. Expertise is required in areas like information security management, auditing and forensics. In order to diminish the lack of an adequate human resource base, both in Government but also in the private sector, the Government will continuously coordinate cybersecurity programs and promote information security career development.

The Digital Uganda Vision aims to reach universal digital literacy and comprehensive utilization of e-services. Thus, public sector institutions need to hire skilled information security officers able to guarantee the availability and safety of e-services, but also to develop the relevant policies and implement them. Information security officers should have a direct reporting line to the Chief Executive, Accounting Officer or Board of the respective MDAs. In order to achieve better accountability, information security officers should not be part of the IT unit or department. **Cybersecurity skills** shall be integrated into **core competencies in public sector**, including Local Governments, as the role and impact of ICT systems is growing in everyday functioning of public sector organisations.

For supporting the cybersecurity competencies and share the information among public institutions, NITA-U as the core implementer of the Cybersecurity Strategy **provides networking facilities** to knowledgeable IT officers across Government MDAs, but also implements capacity building program for IT personnel of MDAs.

With the cost of cybercrime increasing every year across Uganda, the Government is committed to ensure that competent authorities gain better awareness of the threats of cyber- crime and cybersecurity. Therefore, trainings within the Justice Law and Order Sector but also in Defence Sector, will continue.

As the experienced cybersecurity professionals are in high demand, **certification schemas** are crucial steppingstone for almost all careers. Government will coordinate cybersecurity programs and promote **information security career development** in cooperation with the professional associations. In partnerships with academia Government will develop and implement curriculum but also specialized courses that address the required skills.

Government will support and implement professional training courses and skills development schemes for professionals in other sectors as well. First, an assessment of **capacity skills gap at across NCII operators** will be carried out to determine the required resources. In order to promote the establishment of sectoral CSIRT teams, the need to recruit and train experts in the fields of **incident management and forensics and cybercrime prevention** is vital.

3.4.3 Raising public cybersecurity awareness

Digital Uganda Vision promotes universal digital literacy and development, adoption and utilization of e-services. All those using the Internet and related technologies, need to understand the role they play in safeguarding sensitive or personal data. The rise of the Internet demands a **responsible cybersecurity culture**, safe Internet habits and practices to protect personal information online and safely use e-services.

Government will continue to **carry out the awareness programs** to cover various target groups like citizens, MSMEs, children, journalists and others. The aim is to promote trust in e-government, e-commerce services and promote privacy protection and the safe usage of the Internet in general. GoU will broaden the reach of program across age groups and include both individuals, businesses and their associations and create initiatives to continuously inform the public of the current and emerging cybercrime trends, defenses and cyber threats. Annual events like **Cybersecurity Month** to promote cybersecurity awareness will be organized in addition to continuous awareness raising campaigns to improve cybersecurity awareness and literacy of the public focusing on disseminating information about cybersecurity risks and threats. The Government together with the Local Governments will also introduce and design cybersecurity awareness and school-based competitions.

Government of Uganda through NITA-U, together with cross sectoral partners will con- tinue to enhance the **cybersecurity awareness portal**, (besafeonline website) acting as a reference point for cybersecurity awareness-raising materials and initiatives. As indicated in the chapter 1.2, the increased focus is on the enterprises and a dedicated **cyber security web portal** will provide guidelines and awareness-raising materials and initiatives for MSMEs. The cooperation with media companies will be fostered as well and together with Government agencies the guidelines to journalists how to report on cybersecurity incidents and data breaches in a responsible manner will be developed.

3.4.4 Enhance knowledge through research and development

The aspect of Research and Development (R&D) within the Ugandan context ensures the availability of local innovations and solutions that fit current challenges. Building capacity in this area makes us active participants to global cybersecurity solutions. There are good examples of cooperation and initiatives in the R&D area. The Government of Uganda has designed the National ICT Initiatives Support Program (NIISP) and the National Innova- tion Hub to facilitate the creation of an ICT Innovation ecosystem and marketplace for Ugandan innovative digital products like software applications and innovations industry.

The Government will continuously **support Research and Development programs in national universities**, as well as the formation of a national research hub in the area of cybersecurity. The GoU will promote the development and commercialization of intellec- tual properties, technologies, Fourth Industrial Revolution (4IR) and innovations through focused research and development. Through the ICT Innovation Hub, the GoU will foster innovators, incubators, start-ups and the establishment of a cybersecurity cluster to nurture existing companies and create new ventures. The cluster aims to foster innovative technologies and ideas to be commercialized, and to promote an environment for entrepreneurship based on cooperation among industry, academia, and research institutions.

Government support is vital also for enterprises that are undertaking Research and Development in cybersecurity. Therefore, Uganda will **deepen partnerships** for the development of interfaces for research and innovation, and interaction between universities, tertiary institutions such as Uganda Institute of ICT and the local economy, so that skills are linked to market needs. R&D should focus on technologies such as data science, data markets, automation, artificial intelligence, and other state-of-the-art cybersecurity technologies that enable timely detection and response to cyber incidents and threats.

The goal of the GoU is to **provide an ecosystem** comprising of highly skilled professionals, local companies with deep cybersecurity capabilities and strong translational research and development. The ecosystem will ensure a sustainable source of expertise and solutions to support our plans for a resilient national infrastructure and a safer cyberspace.

3.4.5 Action Areas

To promote cybersecurity skills and awareness in Uganda, GoU will:

- **Embed cybersecurity into all stages of education**
  GoU will incorporate cybersecurity as a core learning area at the earliest levels of our education system as well as a specialized area at university and tertiary levels for professionals.

- **Improve expertise, skills and competencies**
  GoU will continuously coordinate cybersecurity programs and promote information security career development by developing specialized courses and curricula, supporting certification schemas, providing networking facilities and support trainings focused on NCII operators, military, law enforcement and Local Governments.

- **Raising public cybersecurity awareness**
  GoU will develop comprehensive program to increase populations awareness. The program will be integrated with the digital (IT) awareness campaigns, in cooperation with telecoms, payment service providers, media companies etc.

- **Enhance knowledge trough research and development**
  The Government will continuously support Research and Development programs in universities and tertiary institutions and promote the development and commercialization of intellectual properties, technologies and innovations through cybersecurity focused research and development. Uganda will promote the research to support digital services to support the use of safest solutions. The GoU will foster innovators, incubators, start-ups andthe establishment of a cybersecurity cluster through the National Innovation Hub to enable innovative technologies and ideas to be commercialized, and to promote an environment for entrepreneurship.

3.5. Active and reliable partner of the international community

- Increasing bi- and multilateral dialogues at the regional level
- Building capacity and confidence through international cooperation
- Promoting calls for action for Responsible State Behaviour in the Cyberspace

Uganda is partnering with various regional and global cooperation initiatives focused on an enhancing cybersecurity and fighting cross-border cybercrime. However, Uganda has yet to sign and ratify the African Union Convention on Cybersecurity and Personal Data Protection (the "Malabo Convention"), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Convention on Cybercrime of the Council of Europe (Budapest Convention). The Ministry of Justice and Constitution- al Affairs (MoJCA) is part of the interagency team which has gathered to accede to the Budapest Convention. Within the planning accession, MoJCA will provide a 24/7 single point of contact for international cooperation against organized and transnational cybercrimes.

Still, in the light of rolling technological innovation to foster the development of the digital economy, against the background of the convergence of information and media services, networks and devices, Uganda acknowledges, that cybersecurity remains essential domain to balance the developments with the need to combat cyber threats on both national and regional level, but also on global arena. Considering increasing evolving threats to cybersecurity, which may constitute serious threats to national, regional, continental and international peace and security, GoU recognizes that international partnerships play essential role in strengthening collective cybersecurity capacities. International partnerships generate opportunities for information sharing and operational collaboration while representing our national interests. Therefore, Uganda remains dedicated on pursuing its active participation in both regional and international forums contributing to strengthening collective cybersecurity efforts and to address combating cybercrime and cyber threats on national, regional and global level.

Uganda on the International arena

Uganda cooperates with following international organizations and forums:

- International Telecommunications Union (ITU)
- Commonwealth Telecommunications Organization
- African Telecommunications Union
- East Africa Communications Organisation (EACO)
- Northern Corridor Integration Projects (NCIP)
- Forum of Incident Response and Security Teams (FIRST)
- Commonwealth Cybercrime Initiative (CCI)

Uganda has signed Memoranda of Understanding on fighting cybercrime with Kenya, Rwanda and South Sudan under the Northern Corridor Integration Projects (NCIP).

Hence, the Strategy aspires to guide global and regional engagements of Uganda across cyber affairs to maintain peace and security. Uganda will invest on coordinating and on establishing the national cooperation forums and formats to develop constructive and favorable international collaboration avenues of mutual interest.

Inspired by the Commonwealth Cyber Declaration

Uganda is striving to establishing and developing the foundations for an effective cybersecurity response and capacity building across diplomatic, policy, legislative, regulatory and technical areas to support both national and international peace and stability.

Uganda is committed to take actions to ensure designing a cyberspace that supports economic and social development and rights online.

3.5.1 Enhance Regional Perspective

The African Union (AU) Peace and Security Council has stressed the need for Member States to undertake regular cybersecurity risk assessments. Therefore, Uganda is dedicated to further cooperation avenues with the AU Commission, as well as with the AU Member States, to further enhance the both national and regional cybersecurity capacities, in order to more effectively address cybersecurity challenges and combat cyber-crimes including the abuse and misuse of the internet. The Peace and Security Council is a key pillar of the African Peace and Security Architecture (APSA) and is a standing decision-making organ of the AU for the prevention, management and resolution of conflict. Developing ways for close collaboration among AU Member States and stakeholders, Uganda is dedicated to contribute to the discussions of the African Union Cybersecurity Expert Group (AUCSEG). Further, Uganda follows the AU Mechanism for Police Cooperation (AFRIPOL) and the International Criminal Police Organization (INTERPOL) for its continued technical support to the efforts being deployed by the AU Member States towards preventing and mitigating the risks posed by cyber crimes. Further, Uganda is proud to host Eastern Africa's Regional Intelligence Unit,that was established following a resolution of the 5th meeting of Peace and Security Council of the African Union held on 2nd of September in Nairobi. Uganda is committed to accelerate its efforts to develop cooperation mechanisms and initiatives with regional partners.

3.5.2 Actively Take International Avenues

International collaboration is key in ensuring the presence of sufficient capacity and mechanisms to handle cyber threats from a foreign adversary as well as provide assistance to international allies. Within the planning accession, MoJCA will provide the 24/7 single point of contact for international cooperation against organized and trans- national cybercrimes.

Participating in International Cybersecurity Diplomatic Negotiations
The United Nations has put efforts to maintain a meaningful conversation on Interna- tional Cybersecurity Diplomatic Negotiations for the last 15 years, mainly through the establishment of the Group of Government Experts (GGE), to discuss international cyber policies. Uganda will follow the Global Approach set up by the ongoing United Nations Open-ended Working Group. Uganda is engaged to contribute to the discussions on responsible state behaviour in cyberspace.

Further, Uganda welcomes joining the Paris Call that invites all cyberspace actors to work together and encourage States to cooperate with private sector partners, the world of research and civil society. The supporters of the Paris Call commit to working together to adopt responsible behaviour and implement within cyberspace the fundamental principles which apply in the physical world.

3.5.3 Building capacity and confidence through collaboration

International collaboration is key in ensuring the presence of sufficient capacity and mechanisms to handle cyber threats from a foreign adversary as well as provide assis- tance to international allies when required.

The effort to improve national cybersecurity will be assisted by participating in regional or international forums that can provide education and training for government, businesses as well as for community. Uganda welcomes and pursues participation in available programs and activities of multilateral organizations that seek to improve and enhance global cybersecurity. Uganda recognizes the continuing need to foster international collaboration and efforts to address cybersecurity issues, including information sharing and assistance. Since mutual legal assistance regime is a part of the **Malabo Convention**, Uganda recognizes the importance to finalise the accession process to develop exchange information mechanisms on cyber threats.

Further, Uganda is dedicated to ensuring its active participation in the international CERT community through the Uganda National CERT and Coordination Center, various cybersecurity communities, organisations and initiatives, to improve and maintain con- nectivity and cooperation with international partners. Further, Uganda intends take full advantage of the various capacity building initiatives of the **Global Forum on Cybersecurity Expertise** (GFCE).

3.5.4 Action Areas

As an active and reliablepartner of international community, GoU will:

- **Increasing both bi- and multilateral dialogues**
  The dialogues with the African Union states and the African Union to support cross-border law enforcement and other mechanisms that serve to achieving better common understanding of the cyber landscape.

- **Building capacity and confidence through international collaboration**
  International collaboration aims to strengthen cyber-capacity and expertise in Uganda for government, businesses as well as for community.

- **Promoting calls for action for Responsible State Behaviour in Cyberspace**
  The initiatives contribute to reducing risks to international peace and security and to the prevention of conflict. The GoU will promote the participation of Uganda's representatives in various international collaboration formats aiming for the responsible state behaviour in cyberspace. Government through the Ministry of Foreign Affairs will keep themselves in the loop on the international discussions, including the implementation of cyber norms and the application of international law in cyberspace, as well as advancing cyber confidence and capacity building.

3.6. Provide an enabling governance framework

- Modernizing the legal framework for NCII
- Fostering information sharing

3.6.1 Cybersecurity Governance and Coordination

Intragovernmental commitment, coordination and cooperation represent core functions of governmental institutions, needed to ensure that the governance mechanisms (i.e., rules) and resources yield the desired outcomes of the Cybersecurity Strategy. The Strategy will be implemented by following the whole of government approach which considers the government as one entity. The model foresees the active collaboration across Government, with enterprises and other stakeholders in the implementation of the Strategy.

Effective communication and coordination ensure that all ministries and government agencies are aware of each other's respective authorities, missions, and tasks. The cybersecurity competent authority ensures that institutions and stakeholders work in a complementary manner.

Government coordination is the prerequisite of the effective implementation of the vision.

The implementation of the Strategy calls for formalizing the national **cybersecurity governance** structure under a multi-stakeholder model. The governance model is based on the principle of shared responsibility. The multitude of stakeholders consists of law- and policymakers, regulators, economic players, educational institutions, technical and business communities, law enforcement, academia, diplomatic and military organizations, and others.

The Cybersecurity Governance Framework is based on the current practice and considers earlier strategic choices. It needs to be stressed that the engagement of the stakeholders across government is both a prerequisite and an essential support for a successful implementation of the Cybersecurity Strategy. Collaboration presents a key to ensure that promises expressed and agreed in the Strategy are measurable and will be delivered in the future.

3.6.2 Roles of authorities

The following institutions are important in creating a favorable institutional framework that will guarantee the coordination and implementation of the strategy.

President chairs the National Security Council.

Parliament will enact the Laws necessary for the enforcing the Cybersecurity Strategy.

Cabinet approves cybersecurity related policies and provides exclusive support for the implementation of Strategy by coordinating the work of MDA's.

National Security Council is the top-level body responsible for security related issues to ensure and maintain internal security, peace and stability. The council is chaired by the President.

Ministry of Information Communications Technology and National Guidance (MoICT&NG)
Ministry's responsibility is to coordinate, provide leadership and oversight in matters of ICT and National Guidance. In relation to cybersecurity, the Ministry is responsible for the development of the relevant policy and legal framework for cybersecurity in Uganda. It also provides support towards the development of relevant legislations for the ICT sector and overall oversight for the ICT sector, including cybersecurity. The MoICT&NG is responsible for the evaluation of the National Cybersecurity Strategy and monitors the implementation of the Strategy.

NITA-U
NITA-U is an autonomous body established under the NITA-U Act 2009 under the general supervision of the MoICT&NG. NITA-U's task is to coordinate and regulate IT services in Uganda. NITA-U also sponsors and hosts the Uganda National Computer Emergency Response Team (CERT.UG/CC) to act as the trusted point of contact, as well as provide central operational coordination for incident response at the national level.

NITA-U is one of the key agencies on implementation of the Cybersecurity Strategy and has the task to coordinate the implementation with relevant other Ministries, Departments and Agencies. In addition, NITA-U is the secretariat of NISAG.

Uganda Communications Commission (UCC)
UCC regulates the telecommunications and broadcasting sub sectors to ensure reliability, redundancy and security of the country's communications infrastructure and consumer protection. It ensures compliance to national cybersecurity laws, policies and standards, and manages the Communication Sector Computer Emergency Response Team.

Ministry of Defence
Ministry of Defence has the responsibility for the protection of the sovereignty and territorial integrity of Uganda. The role of this ministry is to provide cybersecurity protection for all military ICT infrastructures and defend the country's cyberspace against internal and external cyber threats. MoD will establish and maintain the cyber command.

Ministry of Security
Ministry together with the national security agencies under the Ministry is assessing threats for any cybersecurity risk. This entails building capabilities for the protection of Uganda's cyberspace, providing support to fighting cybercrime and sharing intelligence information with relevant actors.

Uganda Police Force
The Uganda Police Force has the responsibility of maintaining Law and Order in Uganda. The role of the Police is to continuously enhance its capacity and capability to effectively investigate cybercrime and provide support to Office of Director for Public Prosecutions.

Inter-ministerial committee
The task of the Inter-ministerial committee is to ensure high level political control and alignment with National Security interests and act as an overall coordinator for the cybersecurity of National Critical Information Infrastructure. The Inter-ministerial Committee is the cooperation format that enables to achieve cross-sectoral agreements and thereby achieve the goals of the current strategy. This committee will include among others the entities listed in this section as well as Uganda National Bureau of Standards, Ministry of Education and Sports, Ministry of Public Service, Financial Intelligence Authority, Office of the Director of Public Prosecution, Justice, Law and Order Secretariat (JLOS), Ministry of Foreign Affairs and Ministry of Trade, Industry and Cooperatives and Bank of Uganda.

The National Information Security Advisory Group (NISAG) acts as coordination mechanism at the operative level that involves all relevant stakeholders. NISAG is responsible for fostering information flow and cooperation amongst all Critical National Infrastructure operators both in the public and private sectors.

National Critical Information Infrastructure (NCII) Regulators
Sectoral regulators supervise NCII operators within their sectors. Thereby they enforce and take lead of the protection of NCII within their sectors. Regulators monitor compliance and performance of operators and support cross sector collaborations and capacity building.

National Critical Information Infrastructure (NCII) Operators
The role of NCII operators is to assess threats and vulnerabilities in their respective areas, analyse and report about cyber incidents and ensure compliance of the relevant cybersecurity laws, policies and standards within their organizations. Another role of NCII operators is to design, implement and test institutional business continuity and Disaster Recovery Plans, and participate in cyber drills.
p
Personal Data Protection Office is responsible for the overall enforcement of the Data Protection and Privacy Act, ensuring applicable administrative, civil or criminal sanctions and penalties, amongst others.

Local Governments
Local governments have a role to plan and implement activities that support the general awareness of cybersecurity threats and guarantee the basic IT skills and cyber hygiene of their employees.

3.6.3 Legislative framework

Collaborative ICT regulatory measures and tools are the new frontier for regulators and policymakers and they should work towards maximizing the opportunities afforded by digital transformation across industries. Uganda aspires to put effort in both harmonizing and developing national norms regulating cybersecurity in any area to achieve the ambitions embarked upon by the Strategy, and to address risk management and proper su- pervisory mechanisms in every sector critical for the functioning of society. For example, there is a need for designing a legislation that will enable and enforce incident reporting both in private and public sector. In order to improve the trust and confidence towards digital transactions and e-services, GoU will enforce the adoption of digital standards, laws and regulation that ensure security of online transactions.

3.6.4 Action Areas

To provide an enabling framework and modernize legal environment, the GoU will:

Modernize the legal framework

The GoU through the Ministry of ICT and National Guidance will revise the legislation and bring it in line with the changing cyber and technological environment, together with the regional and international Conventions to which Uganda has acceded, where applicable. The regulative framework for the protection of NCII will be provided to standardize the security requirements, risk management and incident handling procedures of NCII operators. All NCII operators shall know, understand and follow their responsibilities as a key resource of Uganda's national cybersecurity. The GoU will also harmonize and clarify the responsibilities and supervision of sectoral regulators and specify the cybersecurity aspects in the laws applicable to NCII operators (including the telecommunication, banking and fintech sectors and mobile money providers). On the other hand, the GoU will establish rules and safeguards to protect the users of online services and platforms. Along with the modernization of the legal framework, the digital transformation will be continuously supported by awareness raising measures.

Foster Information Sharing

Appropriate information sharing mechanisms (requirement for the private and public sectors) will be established through legal measures and appropriate protocols through the Uganda National CERT and Coordination Center.

Implementation Matrix

Strategic goal/ pillar	Strategic Action Line	Activity	Output/KPI	Lead Agency	Supporting institutions/ partner	Timeframe				
						Year 1	Year 2	Year 3	Year 4	Year 5
Safe and trusted digital economy	Develop and implement digital identity to facilitate utilization of e-services	Promote the usage of PKI within GoU IT/digital services and applications; enhance the awareness of MSMEs how safely conduct online business and use PKI. Update the standards for electronic signatures.	Security of online transactions is ensured. Standards are updated and specified.	NITA-U	MoICT&NG, UNBS	✓	✓	✓	✓	✓
	Prioritise support for SMEs	Develop dedicated capacity building program for MSMEs to enhance their awareness in cybersecurity and data protection	MSMEs are aware how safely conduct business in online environment.	Ministry of Trade, Industry and Cooperatives	MoICT&NG, Personal Data Protection Office, UCC, NITA-U, the associations of MSMEs	✓	✓			
		Enhance cybersecurity web portal that provides guidelines and awareness-raising materials and initiatives focused on MSMEs.	MSMEs are aware how safely conduct business in online environment.	MoICT&NG	NITA-U. Ministry of Trade, Industry and Cooperatives, the associations of MSMEs	✓	✓	✓	✓	✓
	Expand cybersecurity investments	Support the local cybersecurity industry and continuously expand the government's budget for cybersecurity. Facilitate access to new market segments for domestic cybersecurity companies and promote locally made solutions.	Cybersecurity companies are providing services to the GoU and on the International market.	Ministry of Trade, Industry and Cooperatives, MoICT&NG	NITA-U	✓	✓	✓	✓	✓
Threat preparedness and response	Promote risk assessment practices based on central risk repository	Continuous monitoring and gathering of threat intelligence at strategic and tactical level.	Collection and analysis of the information about threat vectors.	NITA-U, UCC, MoS	NISAG	✓	✓	✓	✓	✓
		Continue the update of National Information Risk Register as both national level and sector oriented cyber risk repository. Improve understanding about current cybersecurity risks to observe and predict trends.	National Information Risk Register is adequate, updated and ready to use for NCII operators.	MoS, NISAG	MoICT&NG, Sectoral Regulators	✓	✓	✓	✓	✓
	Publish regularly Cyber Threat Landscape Report	Publish Cyber Threat Landscape Report, based on threat intelligence and incident information, to improve cyber risk awareness and establish appropriate cybersecurity measures.	Ability of MDAs, NCII operators and MSMEs to detect cyber risks, measure the risk levels and establish appropriate risk controls and mitigation measures has been improved.	NISAG	Sectoral Regulators, CERTs	✓	✓	✓	✓	✓

Strategic goal/ pillar	Strategic Action Line	Activity	Output/KPI	Lead Agency	Supporting institutions/ partner	Timeframe				
						Year 1	Year 2	Year 3	Year 4	Year 5
Threat preparedness and response	Develop central incident register and sectoral incident scenarios	Establish the mandatory incident reporting for NCII and government sector. Develop guidelines for incident reporting for MDAs and NCII operators.	Requirements and detailed guidelines for incident reporting are established legally.	MoICT&NG	NITA- U, MoJCA, UCC	✓				
		Establish and manage an aggregated national level incident register.	National level incident register is functional.	NITA-U with CERT.UG/ CC, NISAG	Sectoral CSIRTs	✓				
		Prepare national and sectoral incident resolution plans as a part of national emergency planning and crises management.	Preparedness for incidents has risen through establishment of sound incident and crisis management plans.	CII Sectoral Regulators	CII operators, NISAG	✓	✓			
	Strengthen national and sectoral CERTs	Define clearly national working arrangements between the CERTs, police or security authorities for information exchange and incident response	Working arrangements between the CERTs, police or security authorities for information exchange and incident response are established.	MoICT&NG, NITA-U, UPF, Security Authorities, UCC	NISAG	✓				
		Define the minimum operation standards for a CERT and undertake implementation of sub sector CERTs	All sub sector CERTs operating using the same operational standards	NITA-U	MoICT&NG, Security Agencies, UPF					
		Promote the establishment of sector specific CSIRTs	Sector specific CSIRTs are established	NITA-U	MoICT&NG, NITA-U, Sectoral Regulators	✓	✓	✓	✓	✓
	Develop tools for information sharing	Foster inter-agency cooperation between security, law enforcement and other government agencies (Standard Operating Procedures) and establish a Cyber Threat Intelligence information sharing framework ie provide clear rules and safe environment for communication	Threat Intelligence information is shared in a timely manner between relevant agencies.	MoS	MoICT&NG NITA-U, UCC, UPF, Security Authorities, Sectoral Segulators	✓				
		Development and regular update of large-scale cyber incident management plans as a part of national emergency planning and crises management	Country is prepared to resolve and recover quickly from a large-scale cyber incident	Sectoral Regulators	NISAG, MoS, MoICT&NG	✓				
	Establish programs for a capacity building in the risk management	Establish capacity building programs for sectors that have less resources for cybersecurity such as MSMEs, healthcare institutions etc.	Appropriate security measures for different sectors are planned, developed and implemented based on adequate understanding of the risks	NITA-U	MoICT&NG, UCC	✓	✓	✓	✓	✓
		Conduct regular cyber incident and crisis management exercises. Participate in international exercises.	Cyber incident and crises management processes are tested and effective. Uganda experts have participated in international exercises.	NITA-U, MDAs, NCII operators, Sectoral Regulators	MoICT&NG, MoS	✓	✓	✓	✓	✓

Strategic goal/ pillar	Strategic Action Line	Activity	Output/KPI	Lead Agency	Supporting institutions/ partner	Timeframe				
						Year 1	Year 2	Year 3	Year 4	Year 5
Robust cybersecurity ecosystem	Establish a strategic plan on the protection of National Critical Information Infrastructure	Establish a strategic plan on the protection of NCII containing the criteria for service criticality as well as description of impact of service disruption. The plan includes incentives for collaboration with the identified NCII operators and supervision mechanisms. Update the strategic plan regularly based on national level risk assessments.	Supervisory authorities, both central and sectoral, are aware of their roles. NCII operators are informed and aware of the cybersecurity requirements for critical infrastructure.	MoS, MoICT&NG	NITA-U, NISAG, sectoral regulators	✓				
	Promote cooperation and understanding of cybersecurity risks in all critical sectors	Assess mutual dependences of the systems and services of various CNII operators. Share the threat intelligence and encourage the operators to a more informed risk management decisions and thereby advocate the investments in appropriate security measures.	A common threat intelligence is shared and NCII operators apply appropriate security measures based on threat landscape.	MoS, MoICT&NG,	NITA-U, NISAG, Sectoral Regulators	✓				
	Raise the awareness of supply chain security risks	Promote the Security-by-Design practices and address the supply chain cybersecurity issues in the framework of through awareness initiatives. National Information Risk Register is updated and addresses the supply chain cybersecurity issues.	Vendors, products and services with high risk are identified and communicated to NCII operators. National Information Risk Register is adequate, updated and ready to use for NCII operators.	NISAG, NITA-U	Sectoral Regulators	✓	✓	✓	✓	✓
		Start the analysis to develop legally binding accreditation system and develop standards to assess the security of hardware, software and IT services deployed in NCII.	Supply chain cybersecurity issues are addressed in an appropriate level and manner.	UNBS	MoS, NITA-U, UCC, MoICT&NG	✓	✓	✓	✓	✓
	Update of the minimal cybersecurity baseline for NCII operators	Update the requirements for minimum cybersecurity baseline of NCIIs (NISF). Include into the baseline the requirements for information sharing and incident reporting. Establish the rules for regular audit.	NCII operators implement security measures and are audited regularly. NCII operators report their cyber incidents to the central level.	MoS, Sectoral regulators	MoICT&NG, NITA-U, UCC	✓	✓			
	Create effective governance and management structure for protection of NCII	Introduce legal provisions that give the relevant sector regulators the authority and resources to oversee compliance.	Sectoral regulators supervise NCII operators within their sectors and enforce the protection of NCII their sectors.	MoJCA	MoICT&NG, Sectoral Regulators	✓	✓	✓	✓	

Strategic goal/ pillar	Strategic Action Line	Activity	Output/KPI	Lead Agency	Supporting institutions/ partner	Timeframe				
						Year 1	Year 2	Year 3	Year 4	Year 5
Cyber skilled Uganda	Embed cybersecurity into all stages of education	Incorporate cybersecurity in educational curricula across primary, secondary and tertiary levels	Enhanced cybersecurity curriculum is rolled out.	NCDC MoES, MoICT&NG	NITA-U, UCC	✓	✓	✓	✓	✓
		Integrate cybersecurity courses in all computer science and IT programs in higher education, including teaching computer security and forensics as a subject or field of expertise.	Cybersecurity courses are available in computer science and IT programs in higher education.	NCDC, MoES, MoICT&NG	NITA-U, UCC	✓	✓	✓	✓	✓
		Promote collaboration between educational institutions and develop a framework for delivering cybersecurity knowledge throughout the education system, especially in primary and secondary schools	Framework for delivering cybersecurity knowledge throughout the education system is established and educational programs are updated.	NCDC, MoES, MoICT&NG	NITA-U, UCC	✓	✓	✓	✓	✓
	Improve expertise, skills and competencies	Strengthen the capacity of the public sector institutions and conduct cyber hygiene trainings. Provide networking facilities to knowledgeable IT officers across Government MDAs and implement the capacity building program for IT personnel of MDAs and Local Governments.	Employees of the public sector institutions are aware of cyber threats, apply appropriate security measures to their ICT systems and use the online environment safely.	MoICT&NG	NITA-U, Local Goverments	✓	✓	✓	✓	✓
		Create cybersecurity positions such as the Information Security Officer across government institutions. Design the job description and designated trainings for future Information Security Officers in MDAs.	The role of the Information Security Officers in public sector institutions is described. The trainings in the MDAs are conducted.	MoICT&NG, MoPS	NITA-U	✓	✓			
		Conduct trainings within the Justice, Law and Order and Defence Sector on cybersecurity and cybercrime related areas	The trainings to Justice, Law and Order and Defence Sector are conducted and national security in cyberspace is enhanced	MoICT&NG, ODPP, JLOS	NITA-U, UPF	✓	✓	✓	✓	✓
		Promote information security career development and coordinate cybersecurity programs between various educational institutions. In partnerships with academia, develop and implement curriculum but also specialized courses on cybersecurity and provide certification schemas for public and private sector.	Specialized courses and certification schemas on cybersecurity are provided.	NCDC, MoES, MoICT&NG	NITA-U, UCC	✓	✓	✓	✓	✓

Strategic goal/ pillar	Strategic Action Line	Activity	Output/KPI	Lead Agency	Supporting institutions/ partner	Timeframe				
						Year 1	Year 2	Year 3	Year 4	Year 5
Cyber skilled Uganda	Raising public cyber-security awareness	Carry out awareness programs to cover various target groups like general public, MSMEs etc. Produce best practice guides for various communities and sectors, including media companies, and organise annual events like Cybersecurity Week.	Awareness programs are developed and conducted for dedicated target groups with the aim to promote trust in e-government and e-commerce. The general level of the cybersecurity culture is raised and the data breaches are published in responsible manner.	MoICT&NG	NITA-U, USS, Sectoral Regulators, UPF Local Governments	✓	✓	✓	✓	✓
		Conduct capacity skills assessment of NCII operators and develop comprehensive security training and awareness program.	Based on the assessment security training and awareness programs are developed and conducted for dedicated target groups	MoS, NITA-U	NISAG	✓	✓	✓	✓	✓
	Enhance knowledge trough research and development	Support Research and Development programs in universities and promote the development and commercialization of intellectual properties, technologies and innovations through cybersecurity focused research and development and through incubators for startups. Deepen partnerships between universities and private sector and establish collaborations with the ICT and cybersecurity industry to develop security solutions addressing the country's cybersecurity needs.	Incubators for enterprises dealing with the development and commercialization of intellectual properties, technologies and innovations are provided. MoUs between Academia and private sector entities to promote international cybersecurity research.	MoES, Academia MoICT&NG	NITA-U, UCC	✓	✓	✓	✓	✓
			Establishment and management of a cybersecurity cluster to foster an environment for entrepreneurship.	UICT, NITA-U, Universities		✓	✓	✓	✓	✓
Active and reliable partner of international community	Increase both bi- and multilateral dialogues	Map existing partners and memberships of regional and international bodies as well as collaboration formats.	Increased and improved partnerships. Number of regional and international organizations that Uganda is a member of, or partners with.	MoICT&NG	MoFA	✓				
		Establishment of cooperation mechanisms like MoU's with national and international partners to enhance the cybersecurity approach and fight cross-border cybercrime	MoUs with international agencies for mutual collaboration to fight cross border cyber crime are established.	MoICT&NG	MoFA	✓	✓	✓	✓	✓

Strategic goal/ pillar	Strategic Action Line	Activity	Output/KPI	Lead Agency	Supporting institutions/ partner	Timeframe				
						Year 1	Year 2	Year 3	Year 4	Year 5
Active and reliable partner of international community	Building capacity and confidence through international collaboration	Establishing national collaboration formats and networks among network operators, academia and civil society organisations to identify and take on board the needs and interests and to forward national input in forms of political and innovative proposals to the relevant international stakeholders.	Enhanced international collaborations on cybersecurity, and improved participation of relevant national stakeholders in cybersecurity programs and initiatives on wider global arena. Improved access to technical support and outreach.	MoICT&NG	MoFA	✓	✓	✓	✓	✓
		Develop the necessary regulation for Mutual Legal Assistance to guide the cross-border sharing and investigation of cyber-crime.	Comprehensive Mutual Legal Assistance Legislation is developed	MoICT&NG, MoJCA	MoFA	✓				
		Develop a secure information sharing policy to facilitate the cross-border sharing of cybercrime information.	Secure Information Sharing Policy for Government of Uganda is developed and implemented	MoICT&NG, MoJCA, MoS	MoFA, NITA-U, UPF	✓				
	Promoting calls for action for Responsible State Behaviour in Cyberspace	Drive the process of ratification and accession to the Convention on Cybercrime of the Council of Europe (The "Budapest Convention") and the Malabo Convention	Consultations are completed and conventions endorsed	MoICT&NG, MoJCA,	MoFA	✓	✓	✓		
		Participate continuously in cybersecurity initiatives, and in the development of regional and international cybersecurity legislation and regulations.	Enhanced international collaboration whereas cybersecurity is a component of Uganda's foreign policy	MoICT&NG, MoJCA	MoFA	✓	✓	✓	✓	✓
Provide enabling governance framework	Modernizing legal framework	Provide the framework for the management of cyber related risks and attacks. Standardize the security requirements and practices for incident reporting and risk handling procedures of the NCII operators.	Revised cyber legislation addressing CNII protection	MoJCA	MoICT&NG	✓	✓			
	Foster Information Sharing	Establishing appropriate information sharing legal mechanisms for private and public sector, including the requirement of incident reporting.	Threat Intelligence information is shared in a timely manner between relevant agencies.	MoS	NISAG, NITA-U, UCC	✓	✓			
	Strengthening protection of a national Critical Infrastructure	Establish transparent and up-to-date legal basis for the protection of NCII, define requirements for security, incident reporting and audit for NCII operators.	Roles and duties of NCII operators are transparent and supervised	MoJCA, MoS	MoICT&NG	✓	✓			

Ministry of ICT & National Guidance
www.ict.go.ug |+256-414-236262