National Cybersecurity Strategy of the Republic of Rwanda 2024-2029

Contents

1 Foreword

The Government of Rwanda (GoR) has invested significantly in Information and Communications Technology (ICT) infrastructure and applications, as a cornerstone for National economic growth. ICT is recognized as a key enabler for economic growth and social mobility and is expected to improve Rwandans' standard of living as part of the Integrated ICT-led Socio-Economic Development Policy and Plan.

Even though the rapid development of ICT in Rwanda promises a positive impact on the nation's economic growth, these technologies have introduced new types of threats which are on the rise globally and are proving increasingly sophisticated. The imminent threat of cyber threats to national security means that GoR must be prepared and in the position to prevent and respond to evolving cyber threats.

Given the heavy investment in the ICT infrastructure to support its economic development goals, it is imperative that infrastructure be resilient and secure against cyber threats. This second National Cyber Security Strategic Plan for Rwanda is published to keep enhancing an environment that shall assure the trust and confidence while using ICT facilities and ensure that Rwanda is self-reliantly able to protect its interests and enforce national security. This policy will guarantee the confidentiality and integrity of information assets and sensitive information of Government, Businesses and individuals.

The Ministry of ICT and Innovation in collaboration with key stakeholders in cyber security especially the National Cyber Security Authority, sector regulators, critical information infrastructure owners, law enforcement agencies, and Academia took the lead in the development of the 2024-2029 national cyber security strategy and action plan, and will periodically review its implementation status to ensure timely execution.

2 Summary

The present document outlines the cybersecurity strategy that the Republic of Rwanda intends to implement in the period 2024-2029. This strategy formalises an ambitious plan that will not only increase Rwanda's cybersecurity level, but that will also support national strategies in other areas of country development (e.g., digitalisation) and that will promote the role of Rwanda in the international cybersecurity arena.

The Strategy revolves around 7 overarching objectives, representing the main areas of intervention:

1. **Consolidate the national cybersecurity framework**: we will make sure that the cybersecurity framework in Rwanda is fit for the challenge and, where necessary, we will amend it, with particular regards to the roles and responsibilities attributed to national entities (institutional aspect) and the laws and legal obligations (normative aspect);
2. **Increase Rwanda's cyber risk management capability**: we will ensure that Rwanda is equipped with the best techniques, tools, and approaches to monitor the threat landscape and to identify, assess, and mitigate cyber-risks;
3. **Make Rwanda ready for cybersecurity challenges**: we will consolidate the operational capability of Rwanda to respond to cyber incidents and emergencies and to minimise the impacts coming for such events;
4. **Protect critical national infrastructures and essential services**: we will support the operators of critical national infrastructures and essential services in their effort to maintain secure their assets and, in doing so, safeguard the wellbeing of Rwanda and its citizens;
5. **Embed cybersecurity in the national culture**: we will push to make cybersecurity an important aspect of education at all levels, helping citizens to understand its importance and giving them the tools to become active participants of cybersecurity;
6. **Build a cybersecurity industry**: we will leverage on our national competences and know-how to establish a cybersecurity industry, making cybersecurity not only more effective but also a revenue stream for Rwanda and its entrepreneurs;
7. **Promote international cooperation**: we will work with international and regional partners to create a safer international scenario regarding cybersecurity, and we will promote a leadership role for Rwanda.

These objectives cover a wide perimeter of intervention. They represent a bold challenge. At the same time, they point to actions that cannot be delayed. Cybersecurity cannot be considered a nice-to-have for Rwanda, nor for any other country. Cybersecurity is an enabler, with impacts in every domain of national governance. Therefore, these objectives are key to ensure that Rwanda can continue its path to national development

These objectives will be pursued by both leveraging the work on cybersecurity that Rwanda has carried out until today and by introducing changes and updates that will help our country to achieve its cybersecurity ambitions.

3 Current state of cybersecurity in Rwanda

3.1 Cyber threats

We are working to create a more digitised and connected Rwanda. This will bring enormous benefit but will also expose our country to several threats coming from the cyberspace. On top of this, important changes to the technological and global scenario are going to affect our internal cybersecurity, such as the rise of artificial intelligence technology. This will provide us with new tools to maintain a safe cyberspace, but it will also be used by malicious actors against us.

Several national institutions are already working to protect Rwanda from such threats. Recent assessments of our risk level show how the work of these institutions is containing the spread of cyber threats while Rwanda continues in its path to digitise itself. However, we must keep our attention level high, especially when it comes to threats against our national critical infrastructures and sectors.

The work of cybercriminals remains a serious threat that is expected to grow. The reach of cybercrime in Rwanda will also increase due to the more widespread access to the internet that the country will achieve in the next years. Ransomware, phishing, online scams, and identity thefts are just a few among the techniques commonly employed by these malicious actors and we need to address them to protect our citizens and organisations.

3.2 Policies and governance

Cybersecurity has been at the forefront of our political agenda for the last years. Our approach to cybersecurity is detailed in several strategic documents that the government adopted in the recent past.

- **III National ICT strategy** (2011): Rwanda's journey toward digitalisation effectively begun in 2001, with the publication of the first National ICT Strategy (NICI I). Cybersecurity was already an important element in NICI I and its 2005 updates, the NICI II. However, only with the NICI III in 2011, the Government of Rwanda clearly identified cybersecurity as a strategic pillar needing dedicated planning and resources.

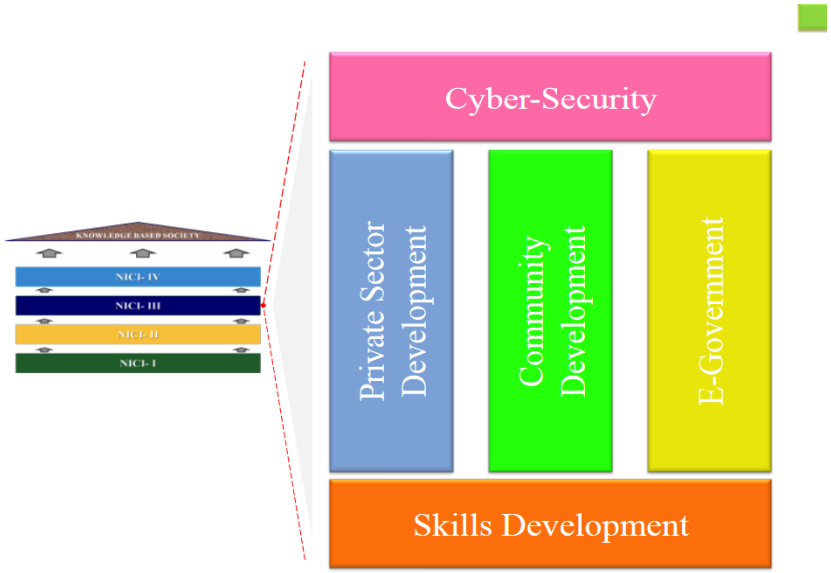

Figure 5: NICI III Framework

- **National Cybersecurity Policy** (2015): This document outlines the previous national cybersecurity strategy, describing the objectives to be pursued. It remains a valid guide, but it now needs to be updated. It continues the on the direction set by NICI III, formalising a structured approach to cybersecurity at the national level.
- **National Strategic Plan** (2015): This document details the actions to reach the objectives identified in the National Cybersecurity Policy.
- **Vision 2050** (2015): This document outlines the path ahead for Rwanda and its citizens and identifies national goals across different sectors and areas of country development.
- **7 years transformation programme** (2017): this document details governmental initiatives to be undertaken by 2024 in line with Vision 2050 and the strategic goals of Rwanda.

Previous contributions provided invaluable support to our cybersecurity posture and were instrumental in setting up specific elements to better govern national cybersecurity. Most notably, Rwanda begun a process of rationalisation of cybersecurity into the normative national framework that already saw the creation of important normative instruments:

- Law n 24/2016 of 18/06/2016 governing Information and Communication Technologies in Rwanda;
- Law n 60/2018 of 22/8/2018 on prevention and punishment of cyber-crimes;
- Law n 58/2021 of 13/10/2021 relating to the protection of personal data and privacy.

However, the changing landscape forces us to continuously update our cybersecurity stance and to rethink our approach to stay ahead of the threats. That why we must continue to work on cybersecurity, leveraging the work and the success built so far.

3.3 Guiding principles

This strategy aligns with previous ones, and recognises the importance of the seven principles already identified in the National Cybersecurity Policy of 2015:

- **National Leadership**: The scale and complexity of cybersecurity requires strong national leadership;
- **Roles & Responsibilities**: All ICT users, including government, businesses and citizens should take reasonable steps to secure their own information and information systems, and have an obligation to respect the information and systems of other users;
- **Public Private Collaboration**: A collaborative approach to cybersecurity across government and the private sector is essential;
- **Risk Based Management**: There is no such thing as absolute cybersecurity. Rwanda must therefore apply a risk-based approach to assess, prioritise and resource cybersecurity activities and their implementation;
- **Rwandan Values**: Rwanda pursues cybersecurity policies that protect the society, the economy and the national vision;
- **International Cooperation**: The cross-border nature of threats makes it essential to promote international cooperation. Rwanda supports and actively contributes to the international cybersecurity activities;
- **Continuous improvement**: we are committed to ensure that Rwanda's cybersecurity posture will keep on increasing;

- **Comprehensiveness**: the National Cybersecurity Strategy shall strive to comprehensively address the need of all of the Rwandan population, Rwandan residents and, when possible, Rwandan partners.

3.4 Cybersecurity roles and responsibilities in Rwanda

Coherently with its journey toward digitalisation, Rwanda has already put considerable effort in cybersecurity. Thanks to this, Rwanda today enjoys a structured approach to cybersecurity, with roles and responsibilities assigned to relevant national actors.

3.4.1 National Cybersecurity Authority

The National Cybersecurity Authority (NCSA) has been established in 2017, by the law No 26/2017[1]. Accordingly, the "The mission of NCSA is to build skills and capacities in cybersecurity with a view to ensuring the protection of the national integrity and security in order to achieve economic and social development."

The NCSA has advisory and coordination responsibilities in the area of cybersecurity. In addition to this, the NCSA enjoys primary responsibilities at the national level in the areas of privacy and personal data protection.

The NCSA enjoys administrative and financial autonomy.

3.4.2 National Computer Security and Incident Response Team

The Rwanda Computer Security Incident Response Team (Rw-CSIRT) is part of the NCSA. It supports public and private institutions affected by cyber incidents. It provides information and recommendations to raise awareness and preparedness in Rwanda, runs early-detection systems to identify and prevent cyber threats, and supports in the response to cyber incidents.

3.4.3 Rwanda Investigation Bureau

The Rwanda Investigation Bureau (RIB) has been established in 2017, by the law No 12/2017[2]. Accordingly, one of the objectives of RIB is to "to prevent and pre-empt criminal acts by identifying and investigating all kinds of physical or cyber-attacks".

The RIB is supervised by the Ministry of Justice and by the National Public Prosecution Authority.

The RIB enjoys administrative and financial autonomy

[1] Law No 26/2017 of 31/05/2017 Establishing the National Cybersecurity Authority and Determining its Mission, Organisation and Functioning.

[2] Law No 12/2017 of 07/04/2017 Establishing the Rwanda Investigation Bureau and Determining its Mission, Powers, Organisation and Functioning.

4 Vision

Our vision: “cyber resilience, digital trust.”

We are committed to align our cyber-vision with the national strategic direction set by the Vision 2050 program. Vision 2050 identifies a mid-term milestone that will lead Rwanda to reach the living standards of upper middle class by 2035. This vision will be achieved by, inter alia, leveraging on the advantages brought by Information and Communication Technology (ICT). However, this reliance on ICT will expose the country to threats coming from the cyberspace that are likely to hinder the achievement of Vision 2050 if neglected.

Therefore, the Rwanda National Cybersecurity Strategy is instrumental in ensuring that Rwanda will achieve what has set out in Vision 2050 as follows:

- It will enable the alignment with other national priorities, strategic objectives and vision;
    - To ensure the protection of economic and social aspirations of the country and national security;
    - To guide a systemic implementation of government cyber priorities, which is deliberated and informed;
- It will enable the alignment with international best practices.

The key strategic pillars of Rwanda’s cybersecurity vision for the next 5 years, will be to:

1. Promote cyber resilience and trust
2. Build the Rwandan cybersecurity industry
3. Enhance cooperation and collaboration

This will secure a drastic improvement in the level of national cybersecurity and will ensure all relevant stakeholders can fully participate in and benefit from the new digital ecosystems that will be created in Rwanda.

5. Strategic Pillars

5.1. Pillar one: Promote cyber resilience and trust

Our digital landscape is rapidly evolving, and cyber threats are growing in scale and complexity, in the quest to achieve greater cyber resilience and trust; defending the systems and assets that constitute our critical infrastructure, and enhancing legislation and regulation are vital to our national security, public safety, and economic prosperity.

This Pillar is designed into 3 priorities and strategic objectives.

Objective 1: Protecting national critical information infrastructure and essential services

Our society relies on several essential services and on the IT infrastructures necessary to deliver said services. Thus, protecting these two elements shall be one of our top national priorities.

On top of that, the growth of Rwanda rests on certain sectors that are strategic for our country's wealth and citizens' well-being. These sectors require particular attention and protection from cybersecurity threats.

Initiative 1: Identify national critical information infrastructure and essential services

We will create a task force involving relevant stakeholders. This task force will have the following purposes:

- Creating a taxonomy and the criteria to identify critical infrastructures, critical information infrastructures and essential services;
- Apply the taxonomy and related criteria to assess the entities that qualify as operators of critical information infrastructures or essential services; and
- Design a monitoring and assessment approach that will ensure the taxonomy, related criteria, and lists of critical information infrastructures and essential services are kept up-to-date.

While pursuing this goal, we will leverage on existing classifications. In particular, we will take into account what is already considered a critical infrastructure/essential service in Vision 2050 (for instance, energy, water, and solid waste management), and we will coordinate with other national stakeholders to build on previous initiatives in this domain.

Initiative 2: Establish baseline security for national critical information infrastructures and essential services

Together with operators and relevant stakeholders, we will identify a minimum baseline security that all critical information infrastructures and essential services must comply with. The adoption of cybersecurity standards that are designed to elevate the resilience of a country's critical cyber assets and reduce corresponding risk levels. This minimum baseline security will cover at least the following aspects:

- Risk management practices and governance;
- Business and service continuity; and
- Implementation and governance of security measures.

We will also produce dedicated guidelines to aid the operators, implement auditing capabilities to verify the compliance levels, and assign roles and responsibilities related to it.

Initiative 3: Protect entities from strategic sectors

In addition to critical information infrastructures and essential services, Rwanda needs to protect with particular care several strategic sectors that, even though might not qualify as critical or essential, are nevertheless crucial for national growth and instrumental in achieving the objectives set by the national leaders.

We will create a task force with involved public and private stakeholders to identify these sectors (e.g., MICE/high-end tourism, ICT, agriculture, etc.) and to design practices to keep the list of sectors up-to-date.

We will adopt measures similar to those for critical information infrastructures and essential services. We will identify minimum baseline security for the identified strategic sectors, including auditing mechanisms to test the security level of the involved entities.

Objective 2: Enhance the legal, regulatory, and governance framework

We will enhance the national legal, regulatory, and governance framework that governs cybersecurity in Rwanda and adapt it accordingly as the cyber threat landscape evolves.

This will cover aspects pertaining to the roles and responsibilities attributed to national entities (institutional framework) and the norms and laws that exist in the area of cybersecurity and cybercrime (normative framework).

Initiative 1: Assess the national cybersecurity landscape

With an ever changing cyber threat landscape, institutions and their governance might need to be fine-tuned to respond to different challenges and needs. We will assess the current institutional framework, past and current projects, and future initiatives with the purpose of identifying gaps or elements that need to be updated and detect overlaps that might lead to unclear responsibilities and waste of resources.

This will involve gaining a thorough understanding of our national cybersecurity landscape and a complete mapping of roles and responsibilities at different levels (national, local, etc.).

Initiative 2: Make the institutional framework more granular

In addition to its layer of national governance, the cybersecurity institutional framework will be enriched through the introduction of additional elements at more granular levels. In particular, the framework should be capable to effectively address cyber threats also at:

- **Sectorial level**: this is of particular importance regarding national critical information infrastructures. However, there are also non-critical information infrastructures that operate in strategic sectors that will require specific cybersecurity measures.
- **Local level**: this will be necessary to close the distance between citizens and cybersecurity responsible authorities. We will work to create dedicated framework at provincial and district levels.

We will update the framework to include roles and responsibilities for these stakeholders, and we will create mechanisms for them to participate and contribute to the collective cybersecurity effort.

Initiative 3: Embed cybersecurity requirements and obligations in the normative framework

Achieving a satisfactory level of national cybersecurity for Rwanda is a responsibility that rests not only on the shoulders of its institutional actors, but requires effort from all its citizens, entities operating inside its territory, and other actors that are involved with Rwanda at different levels. Each one of these stakeholders is to be assigned proportionate duties and obligations in a clear and unequivocal manner.

All the initiatives, roles, responsibilities, and duties need to be codified into one or more national legislation or regulation, to ensure transparency for all stakeholders and help them to understand how to best contribute to the national cybersecurity. We will work with national regulators and governmental actors to enact laws that outline legal requirements such as (but not limited to):

- Obligation to report cyber incidents;
- Mandatory baseline cybersecurity measures for different types of entities;
- Sanctioning mechanisms for non-compliance and breaches of obligations;
- Mandatory cybersecurity certifications for entities and individuals.

In addition, in order to tackle cybercrime and cyber-terrorism, we will work to enhance dedicated legal frameworks that provide law enforcement agencies with the necessary capabilities to detect and investigate potential breaches and the judiciary power with the necessary capabilities to ensure their prosecution.

Objective 3: Make Rwanda ready for cybersecurity challenges

Despite all the efforts to identify and prevent cyber risks and cyber threats, these cannot be completely eliminated. That is why we will work to establish the necessary measures to ensure that Rwanda is prepared to mitigate, respond, and recover from cyber incidents.

Initiative 1: Develop Rwanda's cyber risk management capability

The effectiveness of security and risk mitigation measures decreases when precise and up-to-date information on the cybersecurity landscape is not available to the country. Thus, it is crucial for Rwanda to define – or consolidate when already existing – approaches to not only collect and assess the information about cybersecurity, but also to systematise this information and make it available to concerned stakeholders.

We will define standardized ways to measure cybersecurity risks, including the definition of standard taxonomies and categorisation and, in doing so: (Ref: 5.2.1)

- increase the monitoring capabilities of national entities dealing with cyber risks;
- provide a way to aggregate sectorial cyber risk data into unified indicators of risk exposure;
- facilitate the introduction of tools for real-time monitoring and visualisation of risk exposure;
- provide stakeholders with clearly defined approaches they can rely upon to measure their cyber exposure.

These standard national risk assessment approaches might leverage on existing internationally recognised standards and will be built around clear and easy to understand procedures. Guidance will be provided to further explain these approaches to relevant stakeholders.

Initiative 2: Strengthen national reactive and proactive capabilities against cyber threats

We will work to make Rwanda more effective and efficient in preventing, detecting, and responding to cyber incidents. In particular, we will initiate programs to enhance the current national and sectorial capabilities and to continuously keep these up-to-date.

Building both reactive and proactive capabilities are essential consideration for threat management in the digital age. The ability to respond quickly and effectively to cyber attacks is not enough to protect a country's digital assets and infrastructure, a strategic approach includes both reactive and proactive capabilities that enable the prevention and deterrence of cyber threats.

We will create effective and enduring national cybersecurity programs that include reactive and proactive cyber capabilities to prevent and respond to cyber incidents. Those programs will include:

- Creation of standing practices that can assess the cybersecurity maturity level of Rwanda regularly. This standing capability will both rely on skills and expertise already existing in the National Cyber Security Authority and concerned stakeholders, and on new skills and capabilities that will be introduced to this end;
- Development of a national incident capability that enables response to, and recovery from, cyberattacks in a manner that reduces their impact on society and the economy;
- Establishment of threat neutralization and cyber law enforcement capabilities that protect citizens, the private sector, and the government from cyber criminals;
- Regular measurement and testing of national cybersecurity capabilities to identify exploitable weaknesses and gaps and develop mitigation plans.

One key element to better understand our national cybersecurity level is to gain more information on the threat landscape in which Rwanda operates. Therefore, establishing an effective threat assessment capability will be one of our top priorities. This will be carried out in concert with all relevant stakeholders.

In addition to that, we will establish capabilities dedicated to promoting the sharing of information among national stakeholders, coordinate its collection, and support analysis and assessment (e.g., Information Sharing and Analysis Centres).

Initiative 3: Develop cyber contingency plans

We will work with the national authorities in charge of Emergency Management to develop a plan to respond to national cyber emergencies. The definition of a national cyber emergency aligns with that of Disaster adopted in Rwanda ("a serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources", UNISDR 2008).

The national cybersecurity contingency plan will explain the criteria for activation, the distribution of roles, responsibilities, and tasks, the chain of command, the operational aspects and processes, and the criteria for de-activation.

Moreover, we will work with the most appropriate stakeholders to develop contingency plans dedicated to specific sectors. These sectorial plans will have to satisfy the following needs:

- Provide detailed guidance on how entities belonging to certain sectors or satisfying specific characteristics (such as critical infrastructures and essential services) should act during national cyber emergencies when the national cyber contingency plan is activated;
- Direct the behavior of stakeholders and involved actors in case of sector-wide emergencies not amounting to national cyber emergency. One aspect of particular importance will be to detail the steps necessary to avoid that the sectorial emergency has spill over effects, making it a national cyber emergency (thus requiring the activation of the national cyber contingency plan).

Conducting awareness programs for the developed contingency plans is crucial for their effectiveness, especially among operators of national critical infrastructures. Specific roles and responsibilities will be created regarding the activation of the sectorial contingency plans, and the coordination of the actions provided.

5.2. Pillar two: Build the Rwandan cybersecurity industry

Cybersecurity should not be seen exclusively as an issue to be dealt with. Cybersecurity can also become an opportunity. Creating a national cybersecurity industry should be seen as a strategic imperative to:

- drive innovation;
- make Rwanda a net exporter of cybersecurity products and knowledge and create revenue streams; and
- avoid overreliance on international cybersecurity solutions, tools, methodologies, expertise, etc.

Objective 1: Develop a cybersecurity culture

Our cybersecurity can only be as strong as our weakest link. That is why we are committed to make cybersecurity an element of national culture, available and understood to all national stakeholders, from national leaders to local administrators, from huge corporations to single citizens.

This objective aligns with the goals present in the Vision 2050, in particular:

- Ensuring basic digital literacy for every citizen by 2035; and
- Providing access to internet to 60% of the population by 2035 and 88% by 2050

Initiative 1: Develop a national cybersecurity awareness program

Cyber security awareness promotes foundational understandings of cyber threats and risks, cyber hygiene, and other appropriate response options. It informs citizens about best practices and proactive measures when confronted with cyber risks.

We will work on initiatives that make citizens aware of the cyber risks coming from the use of ICT technologies, equip them with the knowledge and tools to protect themselves online and enhance their capacity in fighting cybercrime. The programs will include, but are not limited to these:

- Awareness programs will be tailored to the capabilities and needs of different population segments. In particular, we will design awareness programs for vulnerable groups such as children, elderly, people with disabilities, etc.
- The cybersecurity awareness programs will be delivered to the population using accessible media, such as newspapers, television, radio, internet, and on-site events.

Initiative 2: Build cybersecurity capabilities for Small-to-Medium Enterprises

We will create initiatives for Small-to-Medium Enterprises (SMEs) to increase their cybersecurity capabilities in a way coherent with the resources at their disposal. In particular, we will work on:

- Developing cybersecurity self-awareness by creating standardised and easy to use assessment models to understand the current cybersecurity maturity;
- Partnering with relevant organisations and stakeholders to fully tap into the SMEs ecosystem and to ensure that cybersecurity measures and initiatives are accessible to SMEs;
- Supporting relevant national authorities and stakeholders in the identification of the best possible way to allocate efforts and resources beneficial for SMEs' cybersecurity;
- Devising mechanisms to ensure the matching between the cybersecurity needs (demand) and the available capabilities (offering) of the job market.

Objective 2: Develop cybersecurity education and capacity building

There is a substantial and growing need to develop a skilled cybersecurity workforce to increase national readiness to respond to threats and adapt to changes in technology.

We will elevate expertise from government, academia, non-profit organizations, and the private sector to generate a workforce with the cyber security skills needed to protect Rwandan cyberspace.

Initiative 1: Develop a national cybersecurity education program

We will design, together with stakeholders in the education space, specific education programs to promote cybersecurity at all levels, from primary school to university. The programs will be tailored to the capabilities and needs of students, with the aim to:

- Provide thorough understanding of basic cybersecurity concepts to children and young adults who regularly use ICT technologies;
- Provide advanced cybersecurity concepts to students of specialised tracks (e.g., technical high-school and universities).

Initiative 2: Establish cybersecurity capacity building programs for the workforce

In addition to formal education and awareness programs, we will create cybersecurity capacity building initiatives for the public sector and for critical information infrastructures and essential services with the purpose to:

- Train people in key areas, such as public officials delivering e-government services, law enforcement personnel, operators of critical information infrastructure and key public sector decision-makers;
- Identify skills 'gaps and vulnerabilities in key areas and provide support to address them;
- Facilitate agreements with neighboring countries and international organisations to deliver cross-border training and exchange of know-how;
- Train specialists to support the national effort toward an integrated e-government experience.

Particular care will be placed upon supporting capacity building for law enforcement and the judiciary, with the purpose of providing them will tools and skills to investigate and prosecute cybercrimes.

Initiative 3: Foster innovation through Research & Development

We will create programs to foster Research & Development (R&D) in the field of cybersecurity. This will include initiatives such as national research grants, incentives for the research and production of innovative cybersecurity patents, concrete support to international research ventures.

The action will seek support from relevant stakeholders such as (but not limited to):

- National research centres and universities;
- The private sector; and
- International R&D centres of excellence.

Objective 3: Public-private partnerships

We will work to facilitate cooperation between the public and the private sectors. Thanks to the inter-sectoral and intergovernmental collaboration initiatives, we will identify specific areas that can be further developed in effective collaboration. In particular, we will work with relevant stakeholders to identify specific elements such as incentives, initiatives to support the encounter of demand and offer for cybersecurity services and products, aid to the market labour, etc.

Integrative alignment and collaboration enable a country to leverage its existing cyber-security strengths and to catalyse the implementation and adoption of new cyber-security measures.

Initiative 1: Promote inter-sectoral and intergovernmental collaboration

We will work to create dedicated initiatives for inter-sectoral and intergovernmental collaboration. These initiatives will be aimed both at facilitating the coordination between these actors and at exchanging views and best practices.

We will first work on securing the commitment of all relevant stakeholders (ministries, public sector managers, trade unions, sectorial organisations, etc.) and we will then move on creating specific initiatives (such as regular meetings, conferences, debates, etc.). These collaborative initiatives will ensure that:

- Relevant cybersecurity stakeholders are timely and regularly updated on the current cybersecurity developments in the country and abroad, so they can address challenges and seize opportunities;
- The risk of duplication of efforts is minimized since all relevant stakeholders will always be up-to-date with the activities and initiatives of other stakeholders;
- Strong bonds will emerge across the national cybersecurity ecosystem and will help organisations to be more effective when responding to time-sensitive issues (e.g., incidents) or when implementing cybersecurity initiatives.

However, participation from the private sector, academia, civil society, and other important segments of society is instrumental for a successful cybersecurity strategy and represents the first line of cyber defence of Rwanda.

5.3. Pillar three: Enhance Cooperation and collaboration

Objective 1: Promote International cooperation

Rwanda cannot pursue national cybersecurity by relying on domestic initiatives alone. The interconnected and networked world in which we live means that cybersecurity issues abroad can become national cybersecurity issues. Therefore, Rwanda should be active on the international cybersecurity scenario and become a champion in cybersecurity and in the fight against cybercrime among regional, African and international cyber communities. The goal should be for Rwanda to be a "Proof-of-concept" for cybersecurity.

Initiative 1: Establish cross-border capacity building

We will leverage on our national cyber capacity building initiatives and expand them to become cross-border exercises by establishing agreements with partners, African countries, and international organisations.

In particular, we will work closely with international partners and organisations to promote incident response and recovery capabilities, such as cross-border cyber contingency plans.

Initiative 2: Create a standing cyber-diplomacy capability

We will cooperate with the national authorities in charge of foreign policy, to ensure that the diplomatic body representing Rwanda's interests abroad is aware of the cybersecurity needs of the country and of how to pursue them at the international level. The personnel of the diplomatic body will be trained to fully engage in regional, African and international expert committees and fora.

On top of that, we will work with relevant stakeholders to provide support and cybersecurity knowledge, either through ad-hoc advisories or through secondment of specialised personnel.

Initiative 3: Promote and strengthen regional, African and international collaboration

We will create mechanisms to encourage Rwandan entities (private and public) to proactively participate in regional, African and international communities and, when possible, to pursue leadership in such international fora. These entities will be our national cybersecurity champions and will benefit from incentives and support.

6. Implementation of the strategy

6.1. Leading implementation authority

The National Cyber Security Authority will be the leading authority in the implementation of this Strategy. It will be responsible for:

- monitoring the overall advancement of Rwanda toward achieving its cybersecurity vision;
- providing regular reporting to national leadership;
- oversighting the activities of other stakeholders that will be involved in the implementation of the strategy;
- acting as a subject matter expert at any stage of the implementation of the strategy.

6.2. Adoption of this strategy at the national level

To ensure the national cybersecurity strategy becomes a pillar of cybersecurity for Rwanda, it will have to be endorsed by the highest political authority. This endorsement will demonstrate to relevant internal and foreign stakeholders the commitment of the national leadership.

Its formal reception into the national legal framework will occur as prescribed by the law.

6.3. Monitoring mechanisms

The National Cyber Security Authority will be tasked to monitor the advancement of Rwanda toward achieving its cybersecurity vision. To this end, the NCSA will establish a formal mechanism to monitor the implementation of the national cybersecurity strategy and, particularly, of the 5-year national cybersecurity action plan. This mechanism will address at least the following elements:

- Policies and procedures to operationalise and formalise the monitoring mechanism. These policies and procedures will have to be endorsed by the national leadership and will grant the NCSA formal authority on its behalf to monitor the implementation of the National Cybersecurity Strategy and the National Cybersecurity Action plan vis-à-vis concerned stakeholders;
- The creation of tools and instruments to ensure that the situation is constantly monitored and that the NCSA always relies on the most current data on the status of the implementation. This will include the design of Key Performance Indicators that will help Rwanda to monitor results in a quantifiable way;
- The establishment of cooperation and consultation mechanisms with concerned stakeholders to ensure the NCSA will do a thorough understanding of the status of single Initiatives and Actions;
- The establishment of a periodic reporting mechanism to the national leadership, to present the adherence of the implementation to the vision and objectives pursued by the strategy.