World Bank
West Africa Regional Communications and Infrastructure
Program (WARCIP)

**THE GAMBIA NATIONAL
CYBERSECURITY STRATEGY**

A PROPOSED FORMULATION

(Draft V1.6)

13 June 2016

Table of contents

Acronyms

ACE	African Coast to Europe (ACE submarine communications cable)
AML	Anti-Money Laundering
CFT	Counter-Financing of Terrorism
CIIP	Critical Information Infrastructure Protection
CIRT	Computer Incident Response Team
CSIRT	Computer Security & Incident Response Team
ECOWAS	Economic Community of West African States
GANAD	The Gambia National Agricultural Database
GDP	Gross Domestic Product
GNCSS	The Gambia National Cybersecurity Strategy
GSC	The Gambia Submarine Cable Company
ICT	Information and Communication Technology
ICT4D	ICT for development
IFMIS	The Gambian Integrated Financial Management System
IMPACT	International Multilateral Partnership Against Cyber Threats (a United Nations-backed cybersecurity alliance through ITU)
ITU	International Telecommunications Union
LMIS	The Gambian Labour Management Information System
MOI	Ministry of Interior
MOICI	Ministry of Information and Communication Infrastructure
NICI	National Information and Communication Infrastructure
NCSA	National Cybersecurity Authority
NCSC	National Cybersecurity Committee
PURA	The Gambia Public Utilities Regulatory Authority
UN	United Nations
WARCIP	West Africa Regional Communications Infrastructure Program
WSIS	World Summit on the Information Society

Preamble

"The Gambia Cybersecurity Strategy" is a project which aims at providing the Government of The Gambia with a formulation of a holistic strategy on cybersecurity.

This document provides such a possible formulation for The Gambia National Cybersecurity Strategy ("GNCSS" or the "Strategy"). It has been developed based on information gathered during the missions conducted in April and May 2016 in Banjul with the support from WARCIP and MOICI, and in dialog with numerous stakeholders from public and private sectors.

Expertise France, Bird & Bird and Civipol have developed this proposed GNCSS so it is built on the current state, plans and aspirations of the country.

It is drafted as a document in such a way that it can be easily and directly implemented in national policy, should the Government of The Gambia want to adopt it as is.

1. Introduction

ICT brings opportunities for economic and social development, and the Government of The Gambia has recognised them through a nationwide strategic plan

Information and communication technology (ICT) is driving a worldwide digital transformation which presents every nations and governments with major opportunities and challenges for their economic and social development. Fully recognizing the importance of ICT by the early 2000's, the Republic of The Gambia has launched numerous initiatives aiming at providing strong foundations conducive to an ICT-led environment beneficial to the socio-economic well-being of the country and its people.

A key political driver is the "**Vision 2020**", which has the ambition to transform The Gambia into a technologically advanced and information rich society.

The vision statement of the **"National Information & Communication Infrastructure (NICI) Policy& Plans"** for The Gambia is "to leverage the benefits of ICT for a people-centered, free market based and export-oriented socio-economic development strategy built on principles of public-private partnership for wealth creation". Its mission is "to achieve higher growth rates in all spheres of socio-economic activities using ICT as a platform to exchange data, information, knowledge and a tool to implement applications and provide services in order to 'leapfrog' several stages of development through a participatory approach in building human resources and a conducive environment".

Within NICI, the "**ICT for development (ICT4D) Action Plans**" set out in that vision and in support of the successive Poverty Reduction Strategy Papers, have led to significant progress in various areas such as Human Resource Development, e-Government, ICTs in Education, Communities, Health, Agriculture, Trade and Tourism, ICT Infrastructure Development and ICT Industry & Services.

More specifically, The Gambia has already implemented several teleservices for its e-administration, such as the Integrated Financial Management System (IFMIS), the Gambia National Agricultural Database (GANAD), the District Health Information System II or the Labour Management Information System (LMIS). E-commerce and mobile money are expanding. In addition, the arrival of the submarine cable ACE and the establishment of a backbone allow all the territory of Gambia to be connected to the global Internet network with high-capacity and reliable bandwidth.

ICT also brings risks, and the Government of The Gambia has responded through a first series of initiatives

The digital development is also accompanied by new threats and risks: it makes the functioning of society very dependent on ICT, often in an irreversible way. Cyber-attacks are often difficult to detect, never cease to grow in number, variety and sophistication, and The Gambia will not remain immune to this threat, as the threat comes from both inside and outside its territory. As a matter of fact, The Gambia has faced different incidents and hacker attacks which compromised government websites.

Because of the increasing interconnection of digital systems through the Internet, the increasing volume of data available and the importance of many processes now digitally handled, the impact of cyber-attacks can be severe. This situation poses a serious threat on the availability, integrity and confidentiality of the systems, data and digital processes, and more generally on the functioning of the Gambian infrastructure and public services.

Fully aware of risks brought by ICT, The Gambia has taken several initiatives for ensuring cybersecurity and so confidence and trust through its ICT-based projects, in coherence with one of the 11 main 'action lines' specified by the World Summit on the Information Society (WSIS): "Building confidence and security in the use of ICTs":

In 2009, the enactment of the **Information and Communication Act** provided The Gambia with rules aiming at ensuring privacy of communications and information and communications services security and setting up electronic signature, and specific legislation pertaining to cybercrime.

The Gambia has also contributed to the building up of regional agreements such as the **ECOWAS Directive on fighting cybercrime** adopted in 2011 and the **African Union Convention on Cybersecurity and Personal Data Protection** adopted in Malabo in June 2014. A CIRT readiness assessment for Gambia has been conducted by ITU in 2011. At last, among others initiatives, some ICT experts, prosecutors and investigators benefitted from cybersecurity or cybercrime training.

Initiative taken by the Government to develop and adopt a national strategy on cybersecurity

Face to the opportunities and challenges highlighted above, the Government of The Gambia has made it a priority to develop and implement a cybersecurity strategy for the country that is consistent with international best practice and aims to strengthen a cross-sector, multi-stakeholder, multi-dimensional concern and not solely a technology problem.

It is of utmost importance to understand that the present Strategy will be implemented in the framework of the NICI Policy & Plans, to contribute to the success of the Vision 2020.

2. Vision

Securing the Gambian cyberspace is an essential pre-requisite for allowing the economic and social development of Gambia and its people to fully benefit from the digital transformation.

In particular, it is a necessary condition so that the NICI Policy & Plans for The Gambia and each of the sectorial plans developed by ministries in application of the plans ICT4D can reach their goals, and more generally, contribute effectively to the Poverty Reduction Strategy and to the strategy of the Vision 2010.

The expected benefits of the Strategy will be a safe and secure cyberspace for the government, business and citizens of The Gambia, a more resilient critical information infrastructure, as well as a better integrated participation in international initiatives related to strengthening cybersecurity and prevent cybercrime across the world.

Another major benefit will be the development of skills and an ecosystem of Gambia-based providers of ICT and cybersecurity services, which will create employment, foster entrepreneurship, thus will strengthen the national economy.

3. Key elements for a successful Strategy

Securing the Gambian cyberspace requires securing each of its ICT systems, networks and critical infrastructure. ("ICT Systems"). Each owner and operator of ICT Systems, whether it is an individual, a NGO, a company or an entity of the public sector, has a responsibility and a way to contribute to the success of the Strategy.

The challenge is that securing ICT Systems requires specific skills that most owners and operators do not have, which results in a need for cybersecurity products and services. It is therefore important for the success of the Strategy that the private sector can respond to this need and that The Gambia can foster the development of a cybersecurity ecosystem.

Because of the nature of the cyber threat, the often complex controls to set up to protect ICT Systems and the severe impacts that could provoke a successful attack in the country, it is also necessary for the success of the strategy that The Gambia sets up a cybersecurity centre that concentrates the highest level of expertise in cybersecurity. Such a centre will enhance the resilience of critical infrastructure and monitor the incident response.

The three elements above constitute the core system aiming at securing ICT Systems in the country.

In parallel of this cybersecurity effort, it is also essential for the success of the Strategy that The Gambia has a capacity of investigation and prosecution for fighting cybercrime.

In order to succeed in securing the cyberspace in The Gambia, the fifth key element is that the users and professionals listed in the four previous elements will engage in and benefit from ongoing education programs, training and awareness activities.

The last key element to the success of the Strategy is a national cybersecurity governance scheme, which will make it fully coordinated and operational. The number and the diversity of the actions to be implemented, and the interaction required among these actions, calls indeed for a coordination at national level.

3.1 People and entities mobilised to secure each ICT Systems

Cybersecurity requires that the basic cybersecurity rules are understood, valued and implemented by the people of The Gambia, at home and at work. Public and private entities, and in particular those maintaining or relying upon critical information infrastructure, shall understand and value the necessity to apply enhanced rules.

3.2 People and entities in capacity to provide cybersecurity technology and services

In order to be understood and implemented successfully, cybersecurity rules require that there are providers and users: on one side The Gambia must be able to rely on people and entities with the capacity to transfer their knowledge and provide support through the delivery of cybersecurity technology and services, and on the other side The Gambia need people and entities with the interest and capacity to apply these rules and use such technology and services.

This calls for the development in The Gambia of an ecosystem of providers and users of cybersecurity solutions and services, enabling public and private entities and particularly operators of critical information infrastructure to secure their ICT Systems.

This ecosystem will create a virtuous circle for the cybersecurity of the whole Gambia, will support the efficiency of ICT4D plans and will foster the creation of employment.

3.3 The GM-CSIRT to operate the national cybersecurity centre

Cybersecurity requires technical knowledge, which calls for the setup of institutions specialised on cybersecurity. A key element will be The Gambia Computer Security & Incident Response Team (GM-CSIRT), which will keep track on ICT vulnerabilities and cyber threats, provide alerts, and help critical infrastructure to respond in case of cyber incident or attack.

3.4 Police forces and Justice to fight against cybercrime

There is no complete cybersecurity as long as those who commit attacks against ICT Systems or through ICT Systems are out of reach of law enforcement authorities and never brought to justice. Fighting against cybercrime is a necessity, in order to limit the threat in the Gambian cyberspace and to contribute to secure the worldwide cyberspace.

The Strategy will ensure that attacks and cybercrime committed in The Gambia or against the ICT Systems will be gradually reported, investigated and prosecuted in a more effective manner.

3.5 Awareness, training & education for all stakeholders

Users and providers of cybersecurity services, experts within institutions in charge of cybersecurity (GM-CSIRT and the national authority in charge of cybersecurity) and the fight against cybercrime (investigators and prosecutors) have all something in common: they will continuously need to grow in expertise through awareness raising, trainings and educations programs. These programs are essential and they will be coordinated through the Strategy.

3.6 A national cybersecurity governance

In order to ensure that the awareness, training and education programs are coordinated, and that the four categories of the stakeholders in The Gambia are gradually empowered and mobilised in an effective manner, a National Cybersecurity Authority (NCSA) and a National Cybersecurity Committee (NCSC) are established to organize the governance and implementation of the Strategy.

To sum up, the success of the Strategy is based on six key elements, also schematically represented in figure 1:

- People and entities mobilised to secure their own ICT Systems

- People and entities in capacity to provide cybersecurity technology and services

- A national cybersecurity centre acting as a centre of competence and an operational centre

- Police forces and Justice in capacity to fight against cybercrime

- Awareness, training & education for all stakeholders

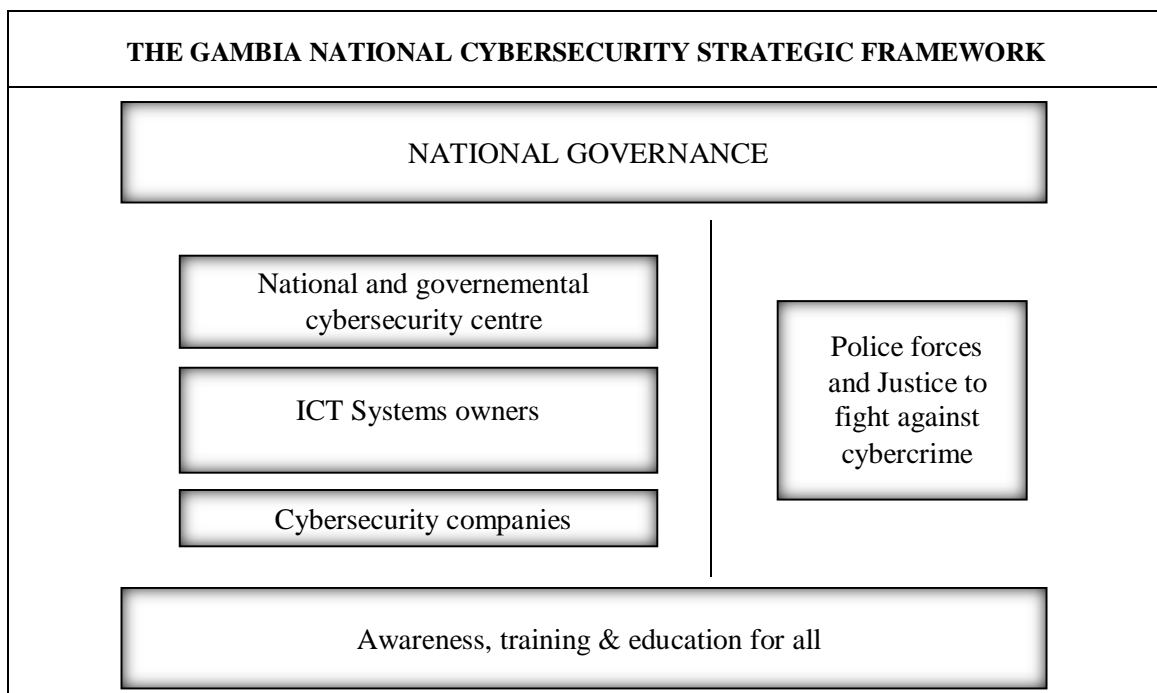- A national cybersecurity governance

Figure 1: the Gambia National Cybersecurity Strategic Framework

4. Principles

The Strategy is based on the following principles:

4.1   Inclusiveness of public policy

Cybersecurity is everyone's responsibility, whether they are users, owners or operators of ICT systems; hence this Strategy is based on the principle that the public policy on cybersecurity of The Gambia shall be inclusive.

All have a role in the major challenge for the protection of digital systems, the prevention and detection of attacks, and the response in the event of a security incident. An inclusive public policy will contribute to make it global, integrated and sustainable.

4.2   Cross-disciplinary approach

Cybersecurity requires the mobilisation of all stakeholders through a cross-disciplinary approach. Applying cybersecurity rules and processes on ICT Systems is not sufficient to ensure true cybersecurity: these rules and processes must be deeply understood by those who are impacted by them, whether they are users, employees or decision makers. In order to get their true participation and support, it is critical to take into consideration the background, constraints and aspiration of each of these groups. This is where a cross-disciplinary approach is useful, as it facilitates the communication between those who provide advice and support, and those who receive such guidance and help.

More generally, the development and implementation of cybersecurity rules and practices need to be organized. Those in charge of cybersecurity shall be given the resources necessary, and the importance of cybersecurity shall be driven to the highest level of management of each organisation.

As such, the Strategy will contribute to align the whole of government, administration and the private stakeholders, businesses, NGOs and citizens towards a coordinated set of actions.

4.3   Lifecycle approach

The constant increase in the number and the impact of cyber-attacks in recent years is a consequence of more connected and more digital economies. The impact of theft of confidential data, malicious access to confidential industrial data, interception of communications or unavailability of systems is significant in the overall economy of a country. For these reasons, it is essential that cybersecurity is considered in the early phase of any initiative or project, and covers the entirety of its lifecycle.

In the daily life of organisations, the culture of lifecycle is not necessarily developed: tasks are assigned and are executed, through a linear process. There may be a review of the quality of the execution, but rethinking the task itself is a different matter.

This linear way of working is well rooted in many organisations but does not sufficiently build on the lessons learned from practical experience, and so does not address the approach needed to build cybersecurity.

A key role of the Committee is therefore not only to advise MOICI on the different phases of the Strategy, but to contribute to develop a "lifecycle culture" at the country level and within the organisation of each member of the Committee.

4.4   Action oriented

This Strategy is action oriented and shall not stay abstract. It is supplemented by an action plan ("Action Plan"), which is regularly updated to adapt to the rapid evolution of cyber threats, and take into account progress made and experience acquired. This Action Plan sets pragmatic targets to be achieved in each of these areas, with a realistic deadline.

4.5   Clarity of roles and responsibilities

Cybersecurity is a multi-stakeholder project, which requires clarity in roles and responsibilities.

The appropriate institutional framework for cybersecurity shall clearly establish and define roles and responsibilities of different authorities in charge of monitoring incidents, preventing cyber-attacks, combating cybercrime and coordinating domestic and cross-border actions in the field of cyber security.

4.6   Threat neutral

This Strategy aims at building a resilient critical information infrastructure and a safe cyber environment against any cyber threat and vulnerability actors, whatever their motivation and goals: cybercriminals, fraudsters, hackers, hacktivists, or Nation States.

It is therefore threat neutral, which means that it is not intended to deal with a specific category of threat and guarantees that it applies usefully to all threats that The Gambia may have to deal with.

4.7   Balance between security and privacy

The legal framework shall address the cyber security challenges while ensuring a proper balance between security considerations and respect of fundamental human rights.

4.8   Implementation

Every plan taken for implementing the NICI Policy & Plans for The Gambia and ICT4D plans should be adapted to take into account this Strategy.

5. Strategic Goals

The Strategy is focused on 5 priority goals.

- The first two priorities are to build capacity of the people, both users and professionals, and provide The Gambia with an institutional framework specific to cybersecurity.

- The next priority is to ensure that ICT Systems are actually protected and made resilient,

- The fourth priority is to provide The Gambia with a comprehensive legal and regulatory framework,

- The last priority is to ensure national and international cooperation.

Further guidance on the implementation of the Strategy is provided in the Action Plan.

5.1. Strategic goal 1: Develop and enhance awareness, training and education

The first priority of the Strategy is the people, who must acquire knowledge and experience in order to successful benefit from the digital transformation brought by ICT.

Indeed, each of the six key elements for a successful cybersecurity strategy requires numerous qualified and trained people to carry out the various tasks to be achieved:
- Cybersecurity professionals are needed to secure the numerous ICT Systems, provide support to owners of ICT Systems, operate the GM-CSIRT and respond adequately to incidents and cyberattacks, as well as educate and train the next generation of cybersecurity professionals;
- ICT professionals must be fully aware of computer hygiene rules and must know how to design, build and administrate ICT Systems in The Gambia in an adequate secure manner;
- Prosecutors and investigators must be sufficiently aware of cybersecurity and cybercrime issues for fighting against cybercrime;

User, at home and at work, need to be aware of cyber threats and basic computer hygiene to protect themselves and their own ICT Systems.

5.1.1 Prepare the next generation of cybersecurity professionals

Cybersecurity is a complex domain that requires to educate and train an increased number of professionals in various fields such as organisation, management and the numerous ICT technologies.

The depth of expertise which is required varies according to the assets to be protected, and the Strategy will pay attention to the need of protecting everyone from the ordinary users to owners of the more complex ICT Systems – in particular those within the critical infrastructure - analysing most sophisticated cyberattacks or tracing cybercriminals. Finding ways to developing deep expertise is a serious challenge, which will not be underestimated.

As a first step, existing IT professionals with interest in cybersecurity will be identified from public and private sector. These individuals will constitute the nucleus group on which the Goal 1 will be built. They will primarily contribute to two paramount responsibilities:
- the development in expertise of the GM-CSIRT and
- set up of a first academic curriculum.

They will be closely linked in a functional network that aims at sharing their theoretical knowledge and practical experience. Their skills should be enhanced as soon as possible by appropriate training and support provided by international organizations or foreign countries.

Furthermore, to ensure the next generation of cyber security professionals, opportunities for additional education will be established, both in the form of higher education as well as on the job training. Support will be given to raise the number of students having completed a training curricula in cyber security and specific actions will be taken to include women into the cyber workforce. A public-private partnership taskforce on cyber security education will be set up which will focus on giving advice about the cyber security curriculum, in relation to the certification of information security experts and the further development of learning modules, among other things. Cybersecurity-specific courses should then gradually be created in universities syllabus.

5.1.2   Enhance cybersecurity knowledge of ICT experts

Securing ICT system is primarily the responsibility of ICT professionals, but in practice they have not received sufficient training on how to secure the systems they are managing. The mission of cybersecurity experts is to support ICT professionals in conducting security assessments and perform most specific or complex cybersecurity controls, which means that ICT professionals must have a minimal level of knowledge in cybersecurity.

Cybersecurity needs to be better included in ICT and must be fully taken into account at each stage of the systems lifecycle, from design phase, deployment, operational phase and withdrawal. Accordingly, academic curricula for ICT professionals will gradually include cybersecurity courses and modules.

5.1.3   Train and educate prosecutors and investigators on cybercrime

In order to improve the efficiency of cybercrime detection and prosecution, the current structure of law enforcement and its organisation of work will be further clarified, the number of personnel dealing with cybercrime will be increased and the capabilities of bodies conducting proceedings to process digital data carriers will be raised. In order to develop capabilities, cooperation takes place with universities and international centres of excellence.

The magistrates and investigators to fight against cybercrime must receive training enabling them to enhance their capabilities and understanding in ICT and its fraudulent use.

5.1.4   Rising public awareness on cyber risks and solutions

The economic damage deriving from cybercrime reduces trust in digital services, and, in a worst-case scenario, could lead to loss of life. Greater awareness among the general public about cybersecurity risks helps to prevent cybercrimes. Greater awareness is achieved by addressing cyber-related topics at all levels of education and informing people based on research and analysis of secure behaviours.

In order to raise the level of awareness of actors operating in cyberspace, attention is paid to introducing actions preventing cyber threats, providing the knowledge needed to identify as well as wisely respond to incidents. Users of e-services are directed to use the most secure solutions and are informed about new technologies and how to securely use these solutions.

5.2. Strategic goal 2: Establish and develop institutional governance and capabilities

The second strategic goal provides The Gambia with an institutional framework that will enable the country to drive successfully the implementation of the Strategy.

5.2.1 National Cybersecurity Authority (NCSA)

MOICI, represented by its Permanent Secretary, is in charge of the oversight, implementation and review of the Strategy.

The Permanent Secretary, assisted by a Deputy who is a Director from MOICI, acts as the National Cybersecurity Authority (NCSA).

The NCSA advises the Government on the initiatives that may be appropriate at a political level for the successful implementation and improvement of the Strategy. In particular, he proposes, or decides within limits delegated by the Government, the appropriate rules, regulations, measures or standards to be implemented to protect critical infrastructures and to ensure security of networks and information systems.

The NCSA monitors the application of the Strategy and ensures its implementation. For this purpose, he can rely on the National Cybersecurity Committee, which has an advisory role regarding the content and implementation of the Strategy. He collects information and recommendations from this Committee.

The NCSA has authority over the GM-CSIRT in all areas of its activity. He ensures that the GM-CSIRT has adequate technical, financial and human resources to carry out its tasks.

The NCSA exercises a liaison function to ensure cooperation within administration and government The Gambia. It consults and cooperates with the relevant national law enforcement authorities whenever appropriate and in accordance with national law.

5.2.2 National Cybersecurity Committee (NCSC)

The National Cybersecurity Committee (NSC) is first and foremost an advisor to the NCSA in charge of cybersecurity for The Gambia on all aspects of the Cybersecurity Strategy, from its elaboration to its implementation and review.

It is therefore of critical important that a variety of interests and expertise are represented and that a balance is established among these interests: public and private sector, technical skills (IT, law…) and development skills (business, education), young and older generations, men and women.

In particular, the NCSC ensures the relevant public and private stakeholders are identified, mobilised and leveraged, in line with the principles listed above.

The NCSA is the Chairman of the Committee and as such calls for the meetings and define their agenda. The NCSC may call and hear any qualified person on the topics listed on the agenda.

The NCSA provides the Secretariat for the Committee.

He has a casting vote in case of a tied vote of the Committee.

The GM-CSIRT, represented by its director, is a permanent member of the NCSC

The National Cybersecurity Committee is divided in 5 subcommittees:
- Enabler, composed of public stakeholders with a cross-sector role (representatives of the Office of the President, MOICI, PURA, CSIRT, NRS).
- Critical Infrastructure, composed of operators of critical infrastructure, notably telecom and financial operators and regulators.
- Law Enforcement, composed of representatives of Ministry of Interior and Ministry of Justice.
- National Security, composed of stakeholders in charge of national security, namely Ministry of Defence and the intelligence agency.
- Civil Society, composed of foundational elements of The Gambia (education, ICT experts, youth, women …).

As cybersecurity is a fast changing phenomenon, composition of the National Technical Committee will be reviewed on an annual basis, in order to ensure that members of the Committee are the most relevant and active stakeholders on cybersecurity.

5.2.3 Gambia Computer and Security and Incident Response Team (GM-CSIRT)

Under the authority of the National Cybersecurity Authority, the Gambia Computer Security and Incident Response Team (GM-CSIRT) acts as the governmental and national operational cybersecurity centre. The GM-CSIRT is also a resource centre for expertise on cybersecurity.

In this role, the GM-CSIRT:
- provides early warning, alerts, announcement and dissemination of information to relevant stakeholders about ICT vulnerabilities, risks and incidents;
- informs the relevant authorities in the event of an incident on an ICT-based system. It assists the affected organisation in identifying the origin of the incident, contain the impact of the incident and supports recovery to normal operations. Unless requested otherwise by the NCSA, the GM-CISRT gives priority to the ICT Systems of ministries and national critical infrastructure;
- provides expertise to cybercrime prosecutors and investigators and preserves digital evidence when it respond to incidents, by taking contact with the relevant law enforcement authorities and by applying their recommendations;
- provides cybersecurity guidance to the national critical infrastructure operators;
- interacts across industry, academia, and the public sector to raise cybersecurity awareness and education and to train stakeholders in the field of cybersecurity;
- establishes connections, exchanges information, participates in cyber drills and more generally cooperates with international CSIRT organizations, e.g. Forum of Incident Response Teams (FIRST), AfricaCERT and the National CSIRT's of its neighbouring countries for enhancing its own overview of the threat landscape and its experience on cyber risks and solutions

The GM-CSIRT has the official mandate to officially act and react to cyber security incidents or threats targeting the Gambia's government ICT.

The capabilities of the CSIRT are regularly assessed and, where needed, enhanced by trainings.

All government entities of The Gambia and national critical infrastructure are required to report serious incidents to the GM-CSIRT.

5.2.4 Setting-up capability on cyber crisis management

The Gambia must be ready to manage societal crisis caused by ICT incidents or cyberattacks. Trainings will be delivered to exercise this capability and enhance the close cooperation between the GM-CSIRT - in charge of coordinating the technical response to the incident - and the management of the societal impact of this incident on the institutions, the public services, the economic life and the people.

5.2.5 Setting-up capability on judicial treatment against cybercrime

As in any field of security, prevention and protection measures will not be sufficient to gain a fully secure environment, and that is even true in the cyberspace, where Gambian interests can be attacked from anywhere in the world. Thus The Gambia has the will to vigorously fight against cybercrime, whether the attacks come from abroad or are conducted from within the country.

The Gambia police forces will set up a capability of cybercrime investigation. The GM-CSIRT will support them as much as possible for education as well as for investigation.

The ministry of justice will ensure that some prosecutors have the awareness of cybercrime, risks and security measures for efficiently achieving the judicial treatment of perpetrators.

National and international cooperation will be enhanced in that field by investigators and prosecutors.

5.3. Strategic Goal 3: Ensuring the protection of information systems, in particular those underlying important services

As mentioned in the key elements for a successful Strategy, securing the Gambian cyberspace increasingly depends on the security of its ICT Systems and services, and the level of protection shall be proportionate to the sensitivity of the information at stake.

Critical infrastructure and ICT Systems must get the highest level of protection and resilience, as their failure or malfunctioning could provoke severe impact on the country, its national security and the economic and social life. These critical ICT Systems, identified under the name of National Critical Information Infrastructure (NCII), are those assets, data, flows or networks of which are vital for achieving the vital services provided by National Critical Infrastructure (NCI).

5.3.1 Identification of The Gambia National Critical Information Infrastructure (NCII)

A regulatory and methodological framework will be officially set up for identifying National Critical Infrastructure (NCI) and within them, National Critical Information Infrastructure (NCII).

NCI and NCII will be selected in the following critical sectors, which can be found in both public and private infrastructure:
i)   banking and finance,
ii)   information and communications,
iii)   power and energy,
iv)   health services,
v)   water and food services,
vi)   national defence and security,
vii)   transport,
viii)   government,
ix)   emergency services.

Furthermore, specific processes and controls specified by NCSA will be implemented by the operators in these sectors, in order to benefit from best practices and increased information sharing.

5.3.2   Ensuring protection and resilience of NCII

In order to provide a minimal level of protection and resilience of National Critical Information Infrastructure, cybersecurity processes and controls will be implemented in mutual consultation between concerned stakeholders under the auspice of the NCSC.

First, these controls will include the obligation to report any sensitive incident or any cyberattack to the GM-CSIRT and the concerned ministry. In a second stage, minimum requirements for compliance will be defined, selected among internationally recognised good practice and standards, such as the obligation to regularly carry out independent cybersecurity audits and to report their results to the NCSC.

Furthermore, attention will be paid to ensure the coherence of the cybersecurity rules with rules specified in the field of physical security.

5.3.3   Foster the adoption of security standards within government and private sector

In order to implement cyber security measures ensuring a more secure cyberspace, a technical standards framework based on international best practice standards will be gradually adopted by both the government as well as the critical infrastructure sector. In order to incentivize entities investing in cyber security and providing information to the Government, positive actions such as revising the tax law or receiving of subsidies will be considered.

5.4. Strategic goal 4: Development of legal and regulatory framework

5.4.1   Establishing appropriate institutional framework

The appropriate institutional framework for cybersecurity shall clearly establish and define roles and responsibilities of different authorities in charge of monitoring incidents, preventing cyber-attacks, combating cybercrimes and coordinating domestic and cross-border actions in the field of cyber security.

5.4.2 Ensuring security of networks and information systems

Appropriate legal provisions shall be made in order to protect networks and information systems with particular attention to national critical infrastructure. Market operators managing critical infrastructure or providing information society services shall be required to adopt appropriate and proportional measures for risk management and recovery in case of incidence. In particular, they should implement appropriate measures for safeguard of the integrity and confidentiality of their networks and information systems and to report serious incidents compromising network and information systems. The respect of such obligation shall be subject to control by a competent authority. Moreover, general requirements for cyber security shall also be observed by public authorities.

5.4.3 Development of a substantive and procedural law on cybercrime

Investigating and prosecuting of cybercrimes should rely upon efficient substantive and procedural law.

The substantive law shall clearly define criminal offences related to ICT:
- Offences specific to ICT (attacks on computer system, computerized data breach etc.),
- Offences committed trough ICT (theft, fraud, money laundering etc.),
- Content related offences trough ICT (child pornography etc.).

Cybercrimes shall be punishable by effective, proportionate and dissuasive sanctions.

The criminal procedural law shall establish the powers and procedures for the purpose of specific investigations or proceedings for cybercrimes. Competent authorities must be enabled to search and seizure computer data, to preserve evidence and computer data as well as impose injunction to communicate or preserve and protect data and evidence.

5.5. Strategic goal 5: National and international cooperation

5.5.1 Promoting active information sharing between public and private entities in The Gambia

In order to enhance visibility into the cyber threat landscape, active information sharing between the GM-CSIRT and the key stakeholders from both public and private sector is encouraged. All information shared will remain confidential between the parties and can be made anonymously.

An appropriate cooperation will be established between competent authorities and bodies in the field of cyber security and law enforcement authority, notably judicial authorities.

5.5.2 **Promoting active international cooperation on cybersecurity**

Protection of critical information infrastructure is enhanced through the participation in the work of international organizations, being represented in the interest groups of partners and allies, and through contributing to the professional development of experts.

Moreover, given the trans-border character of the cyber security, international cooperation is necessary to deal with incidents compromising network and information systems and to investigate and prosecute cybercrimes. For that purpose, various regional and international acts provide means for mutual legal assistance and cooperation that may be put in place in the Gambia (ECOWAS Directive on Fighting Cybercrime, ECOWAS Convention on Mutual Assistance in Criminal Matters, ECOWAS Convention on Extradition, and African Union Convention on Cyber security and personal data protection.

International cooperation will be implemented by the GM-CSIRT as specified in 5.2.3.

5.5.3 **Promoting active international cooperation against cybercrime**

In order to achieve more effective and timely prosecution of cybercrimes with an international dimension, information exchange between countries will be improved, with active participation in various initiatives and projects that are part of the international fight against cybercrime.

6. Implementation

Annual progress reports will be provided to the relevant stakeholders and the action plan will be updated when necessary.

As absolute security is not an achievable goal, the Strategy is rather an ongoing and never ending process. As the Strategy is executed, it must be constantly evaluated and reviewed through a lifecycle process: elaboration, execution and evaluation of the Strategy lead to a new cycle of elaboration and implementation.

Given the ICT progress which implies improvement of techniques used by individuals or groups for malicious purposes, the legal framework shall be subject to periodic review in order to evaluate its adequacy and effectiveness in ensuring cyber security.

7. Glossary

Authenticity:	The property that an entity is what it claims to be.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Business continuity plan, procedures and processes	Plan, procedures and processes set up for ensuring continued business operations.
Computer Security Incident Response Team (CSIRT)	Organisation that receives reports of security breaches, conducts analyses of the reports and responds to the senders. A CSIRT may be an established group or an ad hoc group of experts. Other widely accepted terms exist for CSIRTs, such as CSIRT (Computer Emergency Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team) or SERT (Security Emergency Response Team). A CSIRT can be national, governmental or private. The national CSIRT is the national point of contact for incident response issues, must act as the 'CSIRT of last resort' in case of emergencies, and is the national representation at the international CSIRT communities.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Cyber attack	An attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any digital data, software, computer or ICT services that has value to the organization.
Cyber security incident	IT disruption that limits or eliminates the expected availability of services, and/or is the unauthorized publication, acquisition and/or modification of information". A cyber security incident can involve a real or suspected breach or the unlawful act of exploiting vulnerability. Typical incidents include the introduction of malware into a network, Distributed Denial of Service (DDoS) attacks, unauthorized alteration of software or hardware and identity theft of individuals or institutions. Hacking in general can be considered a security incident unless the perpetrators have been deliberately hired for the specific purpose of testing a computer or network for vulnerabilities.
FIRST	(Forum of Incident Response and Security Teams) the premier organization and global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams. (http://www.first.org)
Information security	Preservation of confidentiality, integrity and availability of information.
Information security incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Incident response and management	The protection of an organization's information by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and then effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems.

Information security forensics	Application of investigation and analysis techniques to capture, record and analyze information security incidents.
information security management system (ISMS)	Part of the overall management system (guidelines, policies, procedures, processes …) set up by an organization for meeting its objectives, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
Information security risk	Potential risk that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.
Integrity	Property of protecting the accuracy and completeness of assets.
National Critical infrastructure (NCI)	Infrastructure and assets the loss or compromise of which could result in a major detrimental impact on national security, national defence, the functioning of the state or essential economic, safety, public health or other social services.
National Critical information infrastructure (NCII)	ICT based infrastructure and assets that are essential for the functioning of National Critical infrastructure
Risk	Effect of uncertainty on objectives. These Objectives can have different aspects (such as financial, health and safety, information security, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk should be characterized by reference to potential events and consequences, or a combination of these, and expressed in terms of a combination of the consequences of an information security event and the associated likelihood.
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk. Risk analysis includes risk estimation.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk management	Set of coordinated activities to direct and control an organization with regard to risk
Vulnerability	A weakness of an ICT asset or control that can be exploited by one or more threats.