REPUBLIC OF SENEGAL

One People – One Purpose – One Faith

Ministry of Communications, Telecommunications, Post and the Digital Economy

SENEGALESE NATIONAL CYBERSECURITY STRATEGY (SNC2022)

November 2017

CONTENTS

ABBREVIATIONS/ACRONYMS

ADIE State IT agency

APIX National agency for promoting investment and major works

ANSD National agency for statistics and demography

ARTP Telecommunications and post regulatory authority

BNLC National anti-cybercrime brigade

CNC National cryptology commission

DDoS Distributed denial of service

DIC Criminal investigation division

DSC Special cybersecurity division (ex BNLC)

CII Critical information infrastructures

KMI Key management infrastructure

CERT Computer Emergency Response Team

CSIRT Computer Security Incident Response Team

CERT/ CSIRT Centre for monitoring for, warning of and responding to IT attacks

MAESE Senegalese Ministry of Foreign Affairs and the Exterior

MCTPEN Ministry of Communications, Telecommunications, Post and the Digital Economy

MEFP Ministry of the Economy, Finance and Planning

MESRI Ministry of Higher Education, Research and Innovation

MFA Ministry of the Armed Forces

MEN Ministry of National Education

MINT Ministry of the Interior

MJ Ministry of Justice

PSE [Emerging Senegal Plan]

PSSI-ES Senegalese government information system security policy

SGPR Secretariat General of the Office of the President of the Republic

SN2025 Digital Senegal 2025

SNC2022 National cybersecurity strategy 2022

TIC Information and communication technology [ICT]

SUMMARY

Wishing to meet its development challenges, Senegal has adopted the Emerging Senegal Plan *(Plan Senegal Emergent (PSE))*, a national strategy which breaks with the approaches of recent decades and puts Senegal on a new route to economic and social development. This new spirit of Senegal, as set out in a vision of "An emerging Senegal in 2035", aims to change how our economy is structured.

Directly in line with this vision and amongst other major efforts, Senegal aims to use new technology and information and communications technology (ICT) in particular as the key drivers of this change.

It is in this context that Senegal has adopted *"Senegal numérique 2025"* (SN2025) ['Digital Senegal 2025"], our national strategy to convert Senegal to a digital society. With this in mind, SN2025 is based on three pillars:

- The legal and institutional framework
- Human resources
- **Digital confidence**

As far as the third of these three pillars of SN2025 ('digital confidence') is concerned, it appears that, for all the players involved, protecting infrastructure, information systems and users, and hence protecting cyberspace as a whole is one of the essential pillars of the ambitions which Senegal sets itself in digital terms.

To guarantee this digital confidence, the Government of Senegal needs to ensure it has the frameworks, tools, knowhow, resources and capacities required not just to eliminate the vulnerabilities in Senegal's existing information systems, but also ensure we are monitoring for cyberthreats, to prevent cybercrime and prosecute it.

The President's order (**https://www.sec.gouv.sn/-PSSI-ES-.html)** on the security policy for the State information systems in Senegal (PSSI-ES) was issued to define the principles and rules to be used an optimum level of security for the government's information systems in accordance with current laws and regulations in force.

This "National Cybersecurity strategy 2022" (SNC2022) sets out Senegal's strategic vision and aims in terms of cybersecurity, reflected in a constant support for the aims and priorities of SN2025.

The key elements of SNC2022 are as follows:

- To evaluate the strategic cybersecurity context in Senegal, including present and future threats;
- The Government's vision of cybersecurity and the strategic aims to be achieved;
- The general principles, roles and responsibilities which can support this strategy;
- The logical framework for implementing it.

Senegal's cybersecurity vision is entitled, **"In Senegal in 2022, a cyberspace of confidence, secure and robust for all.".**

To implement this vision, the Government of Senegal is working to achieve the five strategic aims set out below:

1. *Strategic aim 1: strengthen the legal and institutional framework for cybersecurity in Senegal;*

2. *Strategic aim 2: protect critical information infrastructure (CII) and government information systems in Senegal;*

3. *Strategic aim 3: promote a cybersecurity culture in Senegal;*

4. *Strategic aim 4: strengthen our cybersecurity resources and technical knowhow in all sectors;*

5. *Strategic aim 5: be involved in regional and international cybersecurity work.*

In implementing SNC2022, the Government of Senegal will follow the principles of:

- The rule of law
- Shared responsibility
- A risk-based approach
- Universal access to cyberspace and use it to the full
- Collaboration and cooperation amongst all the parties involved.

With this in mind, the **Government of Senegal will establish a national cybersecurity structure** charged with playing a driving role in cybersecurity issues and implementing and coordinating cybersecurity initiatives in Senegal.

1 INTRODUCTION

Information and communication technology (ICT) is developing rapidly and becoming an increasing part of everyday life in Senegal. In fact, the Senegalese government is actively promoting using ICT generally in everyday life in Senegal via its various national initiatives as described in its strategy SN2025. These initiatives are bringing about a remarkable transformation of Senegal into a digital society in which both public and private sectors use ICT in providing goods and services, conducting transactions and sharing information, enabling people all across Senegal to enjoy an economically wealthier everyday life.

Converting Senegal to digital will involve creating new dependencies, not only on systems, data, infrastructure and cyberspace itself, but also in providing critical services. Any loss of confidence in these systems could harm the digitalisation of Senegal and would limit the benefits of this transformation.

As ICT becomes increasingly integrated in all aspects of life, Senegal will inevitably face growing cyberthreats where troublemakers will continue to exploit our vulnerabilities. These troublemakers are using increasingly sophisticated methods and instruments to hack into information systems, steal, alter or even destroy personal data and public or private institutional data.

Protecting these systems and data thus becomes a national priority as far as Senegal is concerned.

SNC2022 is inspired by the priorities as set out in the PSE, Presidential order 003/PR of 03 January 2017 on PSSI-ES and the aims of SN2025, proposing a global approach in which private individuals, the private sector and government institutions all play their part to the full. In fact, it is these players who will ensure that a dynamic cybersecurity sector grows, along with a skills base which will enable Senegal to keep up to date and monitor the developing cyberthreat environment. This SNC2022 also reflects Senegal's determination and commitment to combat cyberthreats, now and in future.

2 CONTEXT AND SCOPE OF SNC2022

2.1 Strategic context

Since 2004, Senegal has liberalised the telecommunications sector, establishing a legislative and regulatory framework aimed at growing ICT in a secure environment, making the extent and impact of developing technology more transparent in Senegal. In fact, the trends and opportunities observed have increased rapidly since then, with new online technologies, services and applications appearing fast. These developments have also created major opportunities for economic and social growth for Senegal, and will continue to offer major advantages for companies online.

Like any other country, turning Senegal digital will mean relying increasingly on data networks and systems; inevitably, though, these trends will provide more opportunities for individual and groups of troublemakers to compromise these data networks and systems. There are no frontiers in cyberspace, so cybercriminals will continue to intensify their efforts and increase their abilities to target individuals' and organisations' systems across the world, including in Senegal.

2.1.1 Threats

2.1.1.1 Cybercrime

To SNC2022, there are two kinds of cybercrime, as follows:

- Offences which can only be committed using ICT (knowing that these technologies can be used both as the means for committing these offences and as their targets), such as designing and distributing malware with a view to financial and other gains;

- Conventional offences which are perpetrated or aggravated by using ICT.

Cybercrime and cyber-offences are often committed in or against Senegal for financial motives. Those who commit these offences may live in Senegal or anywhere else for that matter; but, even if there are signs of cybercrime and those responsible are identified, it is very often difficult for the forces of law and their international counterparts to pursue offenders, particularly if they are in jurisdictions with limited capacities and/or those which do not have any partnership agreements with Senegal, even though we have divisions specialising in combating cybercrime in our Police and national Gendarmerie, each with their own specialist human and technical resources to help investigate cybercrimes and cyber-offences.

As well as the complex threat of cybercrime which faces Senegal, there is also organised crime working via the 'dark web'. As well as being vulnerable to malware and sophisticated attacks aimed at individuals' and organisations' systems and networks, Senegal is exposed to increasingly aggressive attacks such as ransomware and distributed denial of service (DDoS).

As well as the threats from organised crime groups, there is also a more ongoing form of cybercrime, less sophisticated but more common, against individuals and. Mobile identity theft and fraud are examples of this kind of cybercrime aimed at individuals and organisations via financial transactions.

Although Senegal has Law no. 2008-11 on cybercrime of 25 January 2008, this raises questions and has its own shortcomings, making it less effective. It refers partly to the Criminal Code and partly to the Criminal Procedural Code, for example, which have not themselves been kept up to date with the environment and trends observed in Senegal.

2.1.1.2 'Hacktivism'

Hacktivist groups are generally motivated by a political and social agenda and work on a decentralised basis: so they tend to attack their targets in the interests of specific causes or in pursuit of apparent demands. Although most hacktivist attacks are disturbing by their very nature and include attacks such as DDoS and hijacking websites, they have not mostly caused any major or lasting damage to their targets to date.

2.1.1.3 Internal threats

Internal threats are one of the main risks to any organisation, including those in Senegal. An organisation's staff can access systems and critical data, which is a threat in itself, as they can cause financial and reputational damage by stealing sensitive data. Such staff can also use their knowledge of their organisation to enable or commit attacks designed to stop it working properly. As well as acting deliberately, staff can cause damage unintentionally by not knowing about their organisation's security procedures, particularly by downloading unprotected content, using infected peripherals and opening phishing e-mails. They may also become victims of social engineering via which they may unwittingly allow access to their networks or execute instructions which appear harmless in themselves but which benefit cyber-criminals. With this in mind, the President of the Republic's office, via the National Cryptology Commission (CNC) has taken the offensive and prescribed detailed measures for the security policy for Government information systems in Senegal (PSSI-ES).

2.1.1.4 Cyberterrorism and extremism

Global trends suggest terrorist groups are still considering conducting cyberattacks against countries they target and continue to use the Internet to recruit and radicalise individuals online, be it against Senegal or other countries. Senegal could be a target for such groups one day, so we need to be aware of this threat. Although terrorist groups continue to prefer physical attacks, as economies and societies become increasingly digital worldwide, the probability of highly-qualified terrorist groups or 'lone wolves' increases likewise; and Senegal's reputation could suffer should it turn out that Senegalese acting alone are involved in attacking third countries. All this could be a major threat to Senegal and its interests in the future, so it is vital that we consider this in our strategy.

2.1.1.5 Direct and indirect threats from States

Current trends in cyberespionage and cyberattacks amongst others indicate amongst other things that countries believe increasingly they are targeted, becoming the targets of State-sponsored terrorists seeking to penetrate their governments' systems and networks for political, technological or economic purposes. It is essential that Senegal should be aware of this threat and take steps to mitigate it.

2.1.2 Vulnerabilities

Trends and forecasts globally[1] indicate the rapid proliferation to come of the 'Internet of things' and that Senegal's commitment to digitalising its economy and society suggests there will be new vulnerabilities which can be exploited, even attacked on a grand scale. Indeed, considering the growing devices and processes which are interconnected or connected to the Internet, the vulnerabilities Senegal faces will include those of not having security devices at equipment level, but also threats to interconnected systems on which our society depends.

As networks, systems and software become increasingly vulnerable, it is becoming urgent for our country to develop good practices and cybersecurity processes in all sectors. This need manifested itself since the recent large-scale attacks observed worldwide, like Wannacry in 2017, which hit many governments and businesses worldwide. As most cyberattacks are made exploiting known vulnerabilities and can easily be resolved, it is essential that each country take steps to encourage individuals, enterprises and institutions to take the measures required and invest adequately in reducing these vulnerabilities.

This is consistent with the current situation in Senegal where, despite the work which has been done, we still lack the skills and knowhow to handle the cybersecurity requirements of the private and public sectors. Apart from IT engineers, most staff and officers of most private and public sector organisations in Senegal are unaware just how serious cyberthreats are and are not aware enough of this. Some major private sector organisations like banks and telecoms operators know something about cybersecurity and tend to promote the development of a cybersecurity-oriented culture amongst their staff, particularly in terms of high-risk practices; but there are many organisations, particularly those offering financial services, which do not always take steps which are adequate to their vulnerabilities. Considering there is no coordinated awareness programme at national level aimed at all sectors of Senegalese society, the general public is not aware of cybersecurity issues enough.

One major vulnerability which we currently see in Senegal involves the shortcomings in the field of specialist skills and abilities required to keep abreast with what is happening in cybernetics and adequate technologies to manage the risks and threats involved. It is vital that Senegal deals with these shortcomings.

Many public and private sector organisations in Senegal and individuals also tend to use systems which keep using obsolete or unprotected software versions. In many cases, we find they are using software which suppliers no longer support or for which protection systems no longer exist. Software which is unprotected or obsolete usually suffers from vulnerabilities which those who create cyberthreats search for and exploit.

2.2 Scope of the strategy

SNC2022 explains Senegal's strategic vision and aims in terms of cybersecurity and a commitment to supporting national priorities constantly in promoting converting Senegal to digital. SNC2022 aims to guide the State's actions in terms of cybersecurity by offering the people of Senegal a vision, including public and private sector organisations, civil society and other stakeholders.

[1] *Roundup Of Internet Of Things Forecasts And Market Estimates*, 2016 - https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#368ddbb9292d

SNC2022 covers the whole of Senegal, and announces actions aimed at all sectors of the economy and strata of Senegalese society, including government institutions, private sector organisations and private individuals. The Government will therefore make every effort to ensure that the strategy is implemented for the common good. SNC2022 also proposes improving cybersecurity constantly at all levels for the common good, and defines the context in which Senegal is involved at international level to develop a safe, secure cyberspace.

The strategy defines cybersecurity as protecting information systems (software, hardware and infrastructure), the data they contain and the services they supply or on which they rely against all unlawful access, modifications, obstructions and usage, including actions, whether unlawful or not, due to failing to apply good practice or security procedures properly.

The key elements in SNC2022 are as follows:

- Evaluating the strategic context of cybersecurity in Senegal, including current and future threats;
- The Government's vision for cybersecurity and the strategic aims to be achieved;
- General principles, roles and responsibilities which can reinforce this strategy;
- The logical framework for implementing it.

3 APPROACH

The Government's approach to meet the cyberthreats Senegal faces is based on a precise vision and strategic aims. This approach will strengthen everything which is being done in Senegal to improve companies' cybersecurity by private individuals, public and private sector organisations and civil society and the academic world.

3.1 Vision statement

The strategic vision as proposed represents what Senegal wants for the future. It is rational, all-embracing and forward-looking, analysing the reference situation for cybersecurity[2] and defining the course for the various strategic development aims. To this end, the vision says:

"In Senegal in 2022, a cyberspace of confidence, secure and robust for all"

3.2 Strategic aims

To realise this vision, the Government of Senegal will endeavour to reach five strategic aims as follows:

1. *Strategic aim 1: strengthen the legal and institutional cybersecurity framework in Senegal;*
2. *Strategic aim 2: protect critical information infrastructures (CII) and information systems of the State of Senegal;*

[2] The reference situation in Senegal in terms of cybersecurity, by experts from Oxford University, March 2016

3. *Strategic aim 3: promote a cybersecurity culture in Senegal;*

4. *Strategic aim 4: strengthen resources and technical knowhow in cybersecurity in all sectors*

5. *Strategic aim 5: be involved in regional and international work on cybersecurity.*

3.3 Governing principles

In realising these aims, the Government of Senegal will follow the principles below:

1. **The primacy of law**: SNC2022 will be implemented in accordance with the laws in force in Senegal and international standards to protect rights in Senegal.

2. **Shared responsibility**: SNC 2022 will ensure that everyone involved in the cybersecurity ecosystem in Senegal, such as the authorities, businesses and other organisations and private individuals, commits themselves to protecting their data and IT systems to ensure they are robust and help ensure that other stakeholders' data and IT systems are secure.

3. **A risk-based approach**: the Government of Senegal commits itself to ensuring that everyone involved in the cybersecurity ecosystem in Senegal, such as the authorities, businesses and other organisations and private individuals, adopts a risk-based approach in evaluating and monitoring threats, in responding to incidents in cyberspace or in working in cybersecurity.

4. **Universal access to cyberspace and using it to the full**: the Government of Senegal will work to ensure that everyone involved in the cybersecurity ecosystem in Senegal, such as the authorities, businesses and other organisations and private individuals enjoys cyberspace to the full and uses it to the full to develop encourage more extended socioeconomic development in Senegal.

5. **Cooperation and collaboration amongst stakeholders**: the Government of Senegal recognises the roles and responsibilities of the different players involved in protecting the interests of the Senegalese in cyberspace, and commits itself to working and cooperating with all the stakeholders involved in the cybersecurity ecosystem in Senegal, such as the authorities, businesses and other organisations and private individuals and organisations outside Senegal and with international organisations to protect Senegal in cyberspace.

3.4 Overall approach to achieve these strategic aims

To ensure everything we do in terms of cybersecurity is as harmonised as possible, SNC2022 will be implemented as follows.

In implementing SNC2022, the Government of Senegal will work proactively to ensure that the tools and resources required to ensure the public and private sectors, civil society and anyone living in Senegal are sheltered from cyberthreats. It must also ensure that all the players above can develop the skills and resources and the ability to protect their IT systems and data *per se* dynamically.

4 AIMS TO BE ACHIEVED

The elements below constitute the 'specific aims' and 'actions' to be implemented by 2022 to achieve the 'strategic aims' above and achieve the results desired. They are based on the principles as identified above, and are in line with the approach above:

4.1 Strategic aim 1: strengthen the legal and institutional framework for cybersecurity in Senegal

We need to improve the current legal and regulatory framework in Senegal so we can manage cyberthreats effectively and combat cybercrime, while at the same time ensuring that the new opportunities created by turning Senegal digital become the aces of our economy.

We also need an institutional framework to ensure effective governance of cybersecurity in Senegal, supported by clear functions and roles and well-defined responsibilities and processes.

4.1.1 Specific aim 1.1: strengthen the legal framework of cybersecurity

While Senegal continues transforming itself into a digital society as defined in SN2025, it must at the same time combat various kinds of cybercrime and protect its cyber-interests. Also, given that the cybernetic landscape is developing rapidly and continuously, Senegal will need to review our laws and regulations regularly to ensure they are up to date and reflect emerging trends.

Expected outcomes:

4.1.1.1 Senegal will have an up to date system of laws and regulations in line with developments in cyberspace and international standards, enabling us to combat the malignant cyber activities which threaten our country or which are committed in it.

4.1.1.2 Senegal's system of laws and regulations will provide judicial and security units which have the tools and technologies they need to combat cybercrime.

Actions:

4.1.1.1 Analyse the shortcomings in the laws and regulations concerning ICT and develop adequate tools to improve the cyber-environment and combat cybercrime.

4.1.1.2 Subscribe to regional and international conventions on cybercrime and cybersecurity.

4.1.1.3 Examine and improve the laws and regulations on the procedural powers in investigating cybercrime to prevent, respond to and pursue those who commit those crimes more effectively.

4.1.1.4 Strengthen our laws and regulations on data protection and bring them in line with international standards.

4.1.2 Specific aim 1.2: strengthen the institutional framework to ensure effective governance in cybersecurity

Faced with the increasingly complex threats and challenges cybersecurity involves, the Government of Senegal owes it to itself to provide a strong leadership and effective governance. For this, it is essential that the Government creates an institutional framework which encourages and enables cybersecurity activities to be coordinated quickly and promptly, combined with a coherent, structured approach. This framework will articulate and attribute a set of functions relevant to cybersecurity governance in our country, comprising reviewing SNC2022 regularly, strategic advice and leadership, monitoring cybersecurity initiatives, coordinating detecting and responding to cyber-incidents at national level and preparing private and public organisations and those who have or use IT systems in Senegal in particular.

Expected outcomes:

4.1.2.1 An operational centralised adequate governance structure has been created.

4.1.2.2 A coherent, effective national approach to develop, implement and coordinate cybersecurity operations in Senegal is effective.

Actions:

4.1.2.1 Establish a national cybersecurity structure which will implement SNC2022 and be responsible for developing and coordinating national cybersecurity operations.

4.1.2.2 Implement the CERT/CSIRT national structure in the shape of a unit within the national cybersecurity structure with precise defined functions and responsibilities, including responding to incidents.

4.1.2.3 Identify the relevant public and private sector institutions and use them to make up a consultative committee on cybersecurity whose purpose will be to advise our national cybersecurity structure on matters of strategy.

4.1.2.4 Set up a cyber-defence command and control centre.

4.1.2.5 Strengthen the powers of the defence and security forces and their resources used in combating cybercrime, particularly in using investigation and evidential procedures effectively against crimes and offences committed using digital resources or IT networks.

4.1.2.6 Draw up a cyber-defence strategy which defines our national approach to the cyberthreats facing our national security.

4.1.3 Specific aim 1.3: establish cybersecurity standards, guidelines and an operational and technical framework

Senegal will develop and implement standards and guidelines and operational structures to ensure that public and private sector organisations and those who own and operate critical information infrastructures (CIIs) and our citizens adopt good practices and common actions in the field of cybersecurity. These practices and measures must be founded on the national definition of cybersecurity in Senegal.

Desired outcomes:

4.1.3.1 Clear, understandable and appropriate cybersecurity standards and guidelines are issued, an operational and technical framework, processes and procedures are established and respected in Senegal.

Actions:

4.1.3.1 Issue a set of cybersecurity standards based on international standards but adapted to national level, including on software and writing its source code.

4.1.3.2 Implement an operational and technical management charged with issuing cybersecurity standards and monitoring that they are applied.

4.1.3.3 Promote awareness and implement standards in public and private sectors, amongst SMEs above all.

4.2 Strategic aim 2: strengthen the protection of critical information infrastructures (CIIs) and government information systems in Senegal

The systems and networks which make up cyberspace must be able to keep working during and after cyber-incidents. That is why protecting our Government's systems and networks and those of CIIs are an absolute priority as far as the Government is concerned. The Government will work to ensure that CIIs and Senegalese information systems as a whole can withstand cyber-attacks. For this, it is essential that private sector organisations and their managers and Boards in particular are not just aware of their responsibilities and obligations, but also have the right support to enable them to implement adequate measures to meet cyberthreats.

4.2.1 Specific aim 2.1: ensure critical information infrastructures are protected and that Senegal's information systems are safe

To ensure CIIs are protected and Senegal's IT systems are secure, the Government must first understand what their vulnerabilities are.

Expected outcomes:

4.2.1.1 An exhaustive survey of the vulnerabilities and security levels of the CIIs and Senegal's information systems is available.

4.2.1.2 Design and implement essential measures to improve and showcase how secure Senegal's CIIs and information systems are.

4.2.1.3 Owners of CIIs and information systems' abilities to manage cyberthreats and cyber incidents is improved.

Actions:

4.2.1.1 Establish a directory of CIIs and information systems in Senegal.

4.2.1.2 Define the cybersecurity frameworks, procedures and processes required for any institution which has or manages CIIs and Senegal's information systems.

4.2.1.3 Establish a framework for managing the vulnerabilities of CIIs and Government information system to encourage monitoring them regularly.

4.2.1.4 Conduct tests and other surveillance activities regularly on CIIs and information systems in Senegal.

4.2.1.5 Define minimum and maximum security requirements for Senegal's CIIs and information systems.

4.2.2 Specific aim 2.2: monitor cyberthreats and risk management permanently

The number and gravity of the cyberthreats and cyber-risks facing individuals and organisations continues to grow. Our national cybersecurity structure will be responsible for coordinating managing these cyberthreats and risks, current or emergent, at national level.

Expected outcomes:

4.2.2.1 A coordinating national approach and implementation for managing incidents, supported by a current statement of cyberthreats have been adopted.

4.2.2.2 Senegal now has a better understanding of the size and scale of cyberthreats since cyber-incidents were reported to our national cybersecurity structure

4.2.2.3 Senegal's management of cyber-incidents has been more complete, effective and efficient since a centralised authority was set up for reporting incidents and response to the national cybersecurity structure.

Actions:

4.2.2.1 Define minimum requirements in keeping records of incidents needed to analyse them.

4.2.2.2 Monitor, analyse and manage threats and risks continuously, mitigate, prepare for, respond to and recover from incidents.

4.2.2.3 Set up a national register of risks, regulations and national directives to promote evaluating and managing risks.

4.2.2.4 Create a cybernetic incident log and update it continuously, assess such incidents and offer solutions.

4.2.2.5 Implement data protection and risk management procedures.

4.2.2.6 Design and implement scenarios and programmes for simulating cybersecurity incidents to be used in national drills.

4.2.2.7 Implement national crisis management measures, conduct regular tests by way of cyberattack exercises and evaluate the learnings from these exercises to improve these measures.

4.2.2.8 Create and update continuously an emergency cybersecurity plan defining the roles and responsibilities of the national cybersecurity structure and the defence and security forces in the event of cyberattacks.

4.3 Strategic aim 3: promote a cybersecurity culture in Senegal

Whether digitalising Senegal succeeds depends on whether organisations and individuals have confidence in online services: so the Government needs to work with the public and private sectors to increase their knowledge and understanding of the cyberthreats Senegal and its people currently face. In fact, while a number of organisations, especially in banking and telecoms, are already taking steps to protect themselves, they are still in a minority.

4.3.1 Specific aim 3.1: make all the groups concerned and the general public aware of the security risks in cyberspace.

The Government will run awareness campaigns aimed at both the general public and organisations on cybersecurity risks and how to protect themselves. To do this, it will adopt a range of approaches to optimise the impact of these campaigns, and will work as required in partnership with other organisations and those which offer their customers interfaces exposed to cyberthreats in particular.

Expected outcomes:

4.3.1.1 Individuals and organisations have adopted good practices to reduce the number, severity and impact of the successful cyber-attacks which occur in Senegal continuously.

4.3.1.2 Individuals and organisations understand how important cybersecurity is, what their responsibilities and obligations are and what they need to do to protect themselves, promoting a cybersecurity culture in Senegal generally.

Actions:

4.3.1.1 Conduct a national study to establish how aware people are of cybersecurity at all levels of society and implement a national awareness programme to cover the various target groups.

4.3.1.2 Spread good practice in cybersecurity.

4.3.1.3 Provide mandatory cybersecurity training for senior officers and directors in the private sector so they understand the risks and threats involved better and how to mitigate them.

4.3.2 Specific aim 3.2: establish a reliable environment of confidence to provide government services online and electronic transactions

Spreading online services and government services online and electronic transactions are major elements in working towards a digital Senegal. To achieve this aim, the Government must take up the crucial challenge of the security of services in Senegal. In fact, a minimum

level of security needs to be established so individuals and organisations in Senegal can use digital services in confidence. To do this, the Government will implement specific security measures for these services to encourage people to be confident in them. These include:

- **Authentication**, validating an individual's or entity's identity
- **Confidentiality**, protecting data so only those authorised can access it
- **Integrity**, providing assurance this data has not been modified or falsified
- **Nonrepudiation**, certifying people have been involved in an action or transaction.

More specifically, the Government will amongst other things develop the integration of a key management infrastructure (KMI), IPv6 standard and minimum security standards in designing and deploying government services online and electronic transactions. The Senegalese Government's activities towards this aim are in line with the relevant initiatives defined by SN2025 such as government business architecture or systems for paying taxes and customs duties electronically.

Expected outcomes:

4.3.2.1 Monitoring and minimum cybersecurity requirements are implemented in government services online and electronic transactions, which organisations and people in Senegal and from abroad use fully confidently.

Actions:

4.3.2.1 Encourage the use of KMI security functions, particularly confidentiality, authentication and integrity to create reliable, secure environments for government services online and electronic transactions.

4.3.2.2 Migrate from IPv4 protocol to IPv6.

4.3.2.3 Ensure minimum security requirements are paramount in developing government services online and electronic transactions so people trust in digital.

4.3.3 Specific aim 3.3: promote the use of government services online and electronic transactions

The Government fully recognises the importance of developing knowledge of and explaining the aspects of the security of these services in increasing confidence. With this in mind, the Government will focus on spreading information about the security of these services so people and organisations can choose and make informed decisions about using these services. To understand the concerns of people and organisations in Senegal and respond to them, the Government will set up reliable points of contact which will gather details of users' concerns and decide whether the security aspects of those services meet them. The Government will also ensure that these security facilities are presented to those who use these services in a format and in the language of their choice. In summary, the Government will encourage users, organisations and the government to communicate effectively to maintain confidence in these services.

Expected outcomes:

4.3.3.1 People have confidence in using government services online and electronic transactions in Senegal.

Actions:

4.3.3.2 Set up national points of contact on cybersecurity whose role, amongst other things, will be to gather details of the concerns of those who use government services online and electronic transactions, respond to these concerns and encourage people to use these services.

4.3.3.3 Tell people about cybersecurity measures put in place for government services online and electronic transactions.

4.4 Strategic aim 4: strengthen cybersecurity resources and technical knowhow in all sectors

Competent, qualified human resources in cybersecurity will be needed if an innovative and dynamic ecosystem is to emerge in this specific sector of ICT. Senegal currently has shortcomings in cybersecurity both in education and professional training programmes, staff development and specialist cybersecurity careers. To tackle these, the Government will make developing skills and critical expertise in cybersecurity in Senegal a major priority.

4.4.1 Specific aim 4.1: strengthen resources and technical knowhow in cybersecurity

To realise this aim, the Government will set up a national programme to strengthen cybersecurity resources to secure CIIs, information systems and Internet access networks in Senegal.

Expected outcomes:

4.4.1.1 Senegal will have the skills and expertise to monitor, analyse and manage threats and risks continuously and mitigate, prepare for, respond to and provide feedback on incidents.

Actions:

4.4.1.1 Evaluate national and government institutions' CERT/CSIRT resources and technical knowhow regularly to deal with weaknesses identified.

4.4.1.2 Train and guide national CERT/CSIRT staff regularly so they can handle the most sophisticated cyber-attacks.

4.4.1.3 Train and guide government institution staff regularly so they have the resources and knowhow to prepare for, protect themselves against respond to and recover from incidents.

4.4.1.4 Establish basic cybersecurity training requirements for the private and public sectors.

4.4.2 Specific aim 4.2: strengthen the resources and technical knowhow required to apply laws and regulations effectively

The bodies charged with applying the law will develop the skills and resources required to implement the legal and regulatory framework and pursue those who commit cybercrime by or against anyone or any organisation in Senegal.

Expected outcomes:

4.4.2.1 The organisations responsible for applying the law in Senegal have the skills and resources required to tackle cybercrime.

Actions:

4.4.2.1 Train and guide staff of security services and the courts continuously to strengthen their resources and technical knowhow to tackle cybercrime.

4.4.2.2 Set up mandatory training in digital investigations and handling evidence for staff of security services, the courts and other organisations involved in detecting and prosecuting cybercrime.

4.4.3 Specific aim 4.3: ensure there are enough cybersecurity training/jobs

Considering the roles and responsibilities shared between academia, civil society, the public and private sectors in responding to the shortage of skills in cybersecurity in, the Government will adopt a consistent national approach to develop these skills so there is more technical knowhow about cybersecurity locally. Working with all stakeholders, the Government must increase the number of cybersecurity professionals coming out of Senegal's education system who have the skills required to meet our current needs.

Expected outcomes:

4.4.3.1 There are national education and training programmes in cybersecurity at pre-school, primary, secondary and university level

4.4.3.2 Cybersecurity is recognised as a sector with entrance routes and careers clearly defined.

4.4.3.3 Cybersecurity is an essential element of continuous training for everyone involved.

Actions:

4.4.3.1 Draw up a coordinated programme at national level for education and training in cybersecurity, with a secondary and university arm under the auspices of the ministries concerned.

4.4.3.2 Promote careers in cybersecurity.

4.4.3.3 Evaluate and update programmes and documentation for pre-school, primary, secondary and university levels to include cybersecurity concepts under the auspices of the ministries in charge of education.

4.4.3.4 Draw up partnership contracts between the universities and major colleges at home and/or abroad and the public and private sectors to develop cybersecurity studies, research and training programmes.

4.4.4 Specific aim 4.4: promote the development of the cybersecurity sector in Senegal

The Government will stimulate the growth of an innovative sector in developing reliable cybersecurity products, within which professionals and organisations will enjoy the support, skills and investment required to prosper. To this end, the Government will strengthen the initiatives already under way as part of the SN2025 such as developing digital technology parks, especially that in Diamniadio or again Startup Senegal.

Expected outcomes:

4.4.4.1 Investment in cybersecurity providers and structures has increased significantly.

4.4.4.2 The cybersecurity sector and its contribution to GDP is increasing annually.

4.4.4.3 The Government is supporting cybersecurity providers and structures proactively in a number of ways, including public sector contracts and incentives.

Actions:

4.4.4.4 Promote local and foreign investments in cybersecurity in Senegal and offer incentives.

4.4.4.5 Conduct studies on how cybercrime is affecting Senegal's economy.

4.4.4.6 Support local businesses specialising in developing and delivering cybersecurity solutions.

4.5 Strategic aim 5: be involved in regional and international cybersecurity work

Cyberspace knows no borders, so Senegal will need to work with other countries at regional and international level if it is to help people trust in digital. For the same reason, the Government will also make being involved in regional cybersecurity work a priority, and will work with partners worldwide to meet cybersecurity issues, so helping to contribute to the emergence of a safer cyberspace.

4.5.1. Specific aim 5.1: strengthen international cooperation on cybersecurity issues

The Government of Senegal will seek to reinforce its collaboration and contribution to cybersecurity issues, especially in fighting cybercrime and supporting international cooperation in cybersecurity by taking our place in the cyber-ecosystem globally and encouraging the people of Senegal to behave responsibly.

Expected outcomes:

4.5.1.1 Senegal is actively and effectively involved in regional and international cybersecurity work.

4.5.1.2 Working together more strongly, bilaterally and multilaterally on cybersecurity issues.

Actions:

4.5.1.1 Coordinate Senegal's involvement and strengthen its collaboration with other States and regional and international partners in cybersecurity, especially in fighting cybercrime.

4.5.1.2 Participate actively in regional and international cybersecurity activities, especially in fighting cybercrime.

5 MANAGING AND MONITORING IMPLEMENTING SNC2022

5.1 Roles and responsibilities

The Government of Senegal is fully aware how essential governance and an institutional framework are for cybersecurity, based on the collective responsibility of all stakeholders to protect IT systems, networks, critical installations, data and users. This section defines the roles and responsibilities of the key players involved in implementing SNC2022 clearly.

The **people** who live in Senegal are responsible for taking all reasonable steps to protect the data, software, IT hardware and systems which they own or use in their professional or private life. This is essential for Senegal, given that individuals account for a considerable proportion of our population in cyberspace, and could be an effective line of defence in cyberspace against those who wish us harm, but could also make us vulnerable.

Organisations in Senegal use connectivity and technology as an integral part of their business; they own and operate digital systems, provide digital services and hold personal data. So their responsibility is to protect the resources they have and use and ensure the continuity and security of the digital services they provide. With this in mind, it is vital that businesses and other organisations use all the standards and practices available to protect all personal data they hold and ensure their security and ability to withstand and survive anything which happens to their systems or services.

The **Government of Senegal**'s responsibility is to protect our citizens from harm and bring all criminals to justice. It is also responsible for protecting Senegal against cyberthreats to its national security and critical infrastructures critiques; and, as it provides digital services itself and holds data too, the Government must take strict measures to protect this data and its information systems. As for Senegal's CIIs in providing essential services at national level, and although some of these CIIs or services may be held or operated by the private sector, at the end of the day, the Government is responsible for ensuring that our country is strong and can continue providing the services and functions everyone in Senegal needs. The Government also has a duty to advise and inform organisations and citizens on what they need to do to protect themselves online and issue standards organisations must comply with. The Government must also manage creating an environment which promotes a dynamic, innovative cyber sector in Senegal in which our educational system produces human resources who are able to meet the present and future needs of cybersecurity in Senegal. In a nutshell, the Government of Senegal is responsible for implementing our national cybersecurity strategy. A **monitoring and evaluation committee** chaired by the Minister for Digital Matters will be set up to monitor and evaluate the impact of implementing SNC2022 to assess and resolve any operational obstacles we encounter and assess the impact and results of SNC2022 in the long term.

The authorities, notably the criminal investigation police (police, gendarmes and customs) and the courts will work with our partners bilaterally and multilaterally to strengthen their work in investigating, preventing and prosecuting cybercrime.

Our **national defence forces (armed forces)** are responsible for defending Senegal against cyber-threats against our country's security and sovereignty and investigating all threats in the realm of defence, such as cyberterrorism, cyber-warfare etc. Our national defence forces, via our national cyber-defence command and control centre, are responsible for systems for protecting data and infrastructures used in our national defence and work with our national cybersecurity structure to help protect against and prevent cyber incidents at national level and mitigate their effects and survive incidents.

Our national cybersecurity structure will be set up as the central body for cybersecurity in Senegal responsible for implementing SNC2022. It will be responsible for planning, coordinating and implementing cybersecurity initiatives in Senegal. This structure will protect, prevent, mitigate and help everyone in Senegal recover from cyber incidents sur tout le Senegal and advise and assist organisations in Senegal. It will coordinate protecting CIIs and public and private information systems in this country, and develop and ensure they comply with policies, guidelines, standards and good practices. In brief, it will act as a national voice and centre of expertise in cybersecurity. A **structure steering committee** will be set up to create the national cybersecurity structure.

The **national cybersecurity consultative committee** will be created to provide strategic advice on developing and implementing national initiatives in cybersecurity.

The **civil society organisations of Senegal** will work with other stakeholders in the cybersecurity ecosystem in this country to ensure that public and private sector organisations act transparently and responsibly, to strengthen relations between these organisations and individuals and help make Senegalese society aware of cybersecurity issues.

Academics will work with civil society and the public and private sectors to facilitate developing resources and expertise in cybersecurity, helping meet our current and future needs in terms of competent professionals aware of cybersecurity. Academia will also work with the civil society and the public and private sectors to conduct research and development into cybersecurity

Those who **own and operate critical information infrastructures (CIIs) and information systems in Senegal** will be responsible for protecting their information systems, and so must take all necessary steps to protect them against cyber-threats. They must ensure they comply with standards, directives, processes, procedures and frameworks the government of Senegal creates in terms of cybersecurity.

5.2 Monitoring and evaluation

Cyber-threats are developing constantly, so the Government is fully aware that, if SNC2022 is to be implemented successfully, it must have a monitoring and evaluation framework added. Conducted effectively, monitoring and evaluation can be used to devise new measures or update those which exist.

For this major aspect, the Government's approach will be as follows:

5.2.1.1 Establish specific performance goals which can be measured and achieved within set times for different stakeholders responsible for implementing SNC2022.

5.2.1.2 Draw up annual action plans for each project, defining the expected outcomes, the approach to be used in achieving these results and identifying the resources required to ensure they are implemented successfully. These plans will be based on aims, performance indicators and deadlines set as part of the logical framework for implementing SNC2022.

5.2.1.3 Adopt a general monitoring and evaluation plan based on the approach proposed within three (3) months of launching SNC2022.

5.2.1.4 Monitor and evaluate per se the aims and performance indicators as defined in the logical implementation framework and produce provisional evaluation reports.

5.2.1.5 Regular examinations covering developments in realising the results expected, corrective measures and long-term impacts of SNC2022, including:

- Annual reviews
- A mid-term review at the end of year two of implementing SNC2022;
- A long-term review at the end of year four of SNC2022.

6 CONCLUSIONS

The rapid development of cyberspace offers major benefits for accelerating the growth of Senegal's economy; but cyberspace also involves vulnerabilities and growing cybercrime which undermine not only confidence in a digital Senegal but the 'digital Senegal 2025' vision itself.

SNC2022 sets out the approach and commitment at national level to eliminating these vulnerabilities in relation to CIIs and information systems in Senegal and fighting cybercrime effectively. In taking this approach, Senegal is committed to being proactive faced with current and future threats by giving ourselves adequate resources.

Implementing SNC2022 will, in fact, make Senegal more mature in terms of cybersecurity, not only through understanding and managing the vulnerabilities, threats, risks and incidents which cyberspace involves better, but also growing the cybersecurity sector with an expertise and highly competitive local products.

By 2022, everyone involved in society will be using cyberspace properly, using all its potentiality in full confidence.

7 ANNEXE A – LOGICAL FRAMEWORK FOR IMPLEMENTING SNC2022

This annexe presents the key elements necessary to implement this strategy optimally:

- Strategic aims: substantive long-term aims which will help achieve the vision;
- Specific aims: the steps required to achieve each strategic aim;
- Strategies/actions: what needs to be done to achieve the specific aims;
- Deliverables/outcomes: results of action taken;
- Lead and support agencies: the institutions or bodies which are principally responsible for realising each aim and those which provide supporting services.
- Deadline: period in which deliverables/outcomes will be produced and/or strategies or actions implemented.
- Key performance indicators: indicators, data measurements and trends which must be monitored to assess how we are progressing in implementing the strategy.
- Funding sources: identifying potential funding structures for implementing strategy.

Strategic aim 1: strengthening the legal and institutional framework for cybersecurity in Senegal

Specific aim 1.1: strengthening the legal framework for cybersecurity

Expected outcomes:

- Senegal will have an up to date framework of laws and regulations both in line with developments in cyberspace and with international standards, enabling us to combat the cyber-activities of our country's enemies and those which are committed within our country effectively.
- Senegal's laws and regulations will provide for criminal investigation and security units with the right tools and technologies to do their job fighting cybercrime

Strategies/ actions	Lead and support agencies	Deliverables/ results	Due date	Key performance indicators	Possible funding sources	Estimated cost (XOF)
1.1.1 Analyse the shortcomings in the framework of laws and regulations on ICT and produce adequate tools to improve the cyber environment and fight cybercrime.	LEAD MCTPEN CNC	A study which identifies the shortcomings in the framework of laws and regulations on ICT in terms of cybersecurity. Adequate tools to improve the cyber environment and fight cybercrime.	June 2018	How far has the framework of laws and regulations been reviewed? Have adequate tools been adopted to improve the cyber environment and fight cybercrime? How much more effective is the framework of laws and regulations?	LEAD MCTPEN	35,000,000

1.1.2 Sign up to international and regional conventions on cybercrime and cybersecurity	LEAD MCTPEN	International and regional conventions on cybercrime and cybersecurity	December 2018	How far have international and regional conventions on cybercrime and cybersecurity been applied? How effective are international and regional conventions on cybercrime and cybersecurity?	LEAD;	10,000,000
1.1.3 Examine and improve laws and regulations on procedural powers in investigating cybercrime to prevent, respond to and prosecute those who commit such crimes more effectively	LEAD MJ MFA MINT	Laws and regulations on procedural powers in investigating cybercrime	June 2018	How effective are laws and regulations? How far are laws and regulations being applied? How much room is there to improve laws and regulations?	LEAD MJ	35,000,000

1.1.4 Strengthen framework of data protection laws and regulations and bring in line with international standards.	LEAD MCTPEN; MJ; CDP National cybersecurity structure	Framework of data protection laws and regulations	September 2018	How effective is the framework of data protection laws and regulations? How far is the framework of data protection laws and regulations being applied? How many organisations are there which adopt and implement framework of data protection laws and regulations?	LEAD MCTPEN; MJ; National cybersecurity structure	25,000,000

Specific aim 1.2: strengthen institutional framework to ensure effective governance in cybersecurity

Expected outcomes

- An operational centralised adequate governance structure has been created.
- There is a consistent, effective national approach to developing, implementing and coordinating cybersecurity operations in Senegal.

Strategies/ actions	Lead and support agencies	Deliverables/ outcomes	Deadline	Key performance indicators	Potential funding sources	Estimated cost (XOF)
1.2.1 Establish a national cyber-security structure which will lead implementing SNC2022 and be responsible for developing and coordinating national activities in cybersecurity.	LEAD SGPR MCTPEN	National cyber-security structure operational	September 2018	Publish text Operationalise national cyber-security structure	LEAD SGPR MCTPEN	950,000,000
1.2.2 Implement national CERT/ CSIRT as a unit within the national cybersecurity structure with precise functions and responsibilities, including responding to incidents	LEAD SGPR MCTPEN	National CERT/ CSIRT as a unit within the national cybersecurity structure	December 2018	Publish text Operationalise national cyber-security structure	LEAD SGPR MCTPEN	

1.2.3 Identify relevant public and private sector institutions and create a consultative cybersecurity committee to provide strategic advice to national cybersecurity structure	LEAD MCTPEN	Consultative cybersecurity committee	December 2018	Publish text Operationalise committee	LEAD MCTPEN	15,000,000
1.2.4 Set up a cyber-defence command and control centre	LEAD Min Armed Forces (MFA)	Cyber-defence command and control centre	December 2018	Publish text Operationalise cyber-defence command and control centre	LEAD Ministry for the Armed Forces (MFA);	900,000,000
1.2.5 Give defence and security forces more powers and resources to fight cybercrime, particularly in using effective investigation and evidential tools in dealing with crimes committed with digital tools or IT networks	MFA; MJ; MINT ADIE	Mandate and role of defence and security forces in fighting cybercrime, particularly in using investigation tools effectively and establishing proof of offences	Publish text: December 2018	Publish text How far is text being applied?	MFA; MJ; MINT	35,000,000

1.2.6 Draw up a cyber-defence strategy defining the national approach to cyber-threats to national security.	LEAD MFA	National cyber-defence strategy	December 2018	How far is national cyber-defence strategy being applied?	LEAD MFA	3 5,000,000

Specific aim 1.3: establish cybersecurity standards and guidelines and an operational and technical framework

Expected outcomes

- Comprehensible, appropriate cybersecurity standards have been issued and guidelines, an operational and technical framework, processes and procedures are established and complied with in Senegal

Strategies/ Actions	Lead and support agencies	Deliverables/ results	Due date	Key performance indicators	Possible funding sources	Estimated cost p.a. (XOF)
1.3.1 Issue a set of cybersecurity standards taking account of inter-national standards and adapted to national level, including for software and developing its source code.	National cyber-security structure MCTPEN CNC ADIE	A set of standards on cybersecurity reflecting intern-national standards and adapted to national level	December 2018	How far is the set of cybersecurity standards being applied?	National cybersecurity structure; MCTPEN	15,000,000
1.3.2 Set up an operational and technical framework charged with issuing cyber-security standards and monitoring their application.	MCTPEN; Private sector; National cyber-security structure	An operational and technical framework charged with issuing cyber-security standards and monitoring their application.	December 2018	How far is an operational and technical framework being applied?	MCTPEN; Private sector; National cyber-security structure	10,000,000

1.3.3 Promote awareness and implement standards in public and private sectors, particularly amongst SMEs	MCTPEN; Private sector; National cyber-security structure	A national programme to promote adapting and adopting cyber-security standards	June 2019	How far is the set of cybersecurity standards being applied? How many organisations are adopting and implementing all cybersecurity standards?	MCTPEN; Private sector; National cyber-security structure	10,000,000

Strategic aim 2: improve protection of critical information infrastructures (CIIs) and information systems in Senegal

Specific aim 2.1: ensure critical information infrastructures are protected and safeguard information systems in Senegal

Expected outcomes

- An exhaustive survey of vulnerabilities and levels of security of CIIs and information systems in Senegal is available.
- Create and apply essential measures to improve and showcase the security of CIIs and information systems in Senegal are effective.
- The ability of those who operate and own CIIs and information systems to manage cyberthreats and cyber-incidents has been improved

Strategies/ Actions	Lead and support implementation agency	Deliverables/ outcomes	Timescale	Key performance indicators	Possible funding sources and mechanisms	Estimated cost p.a. (XOF)
2.1.1 Produce a directory of CIIs and information systems in Senegal.	ARTP; ADIE CNC National cyber-security structure	Directory of CIIs and information systems in Senegal.	September 2018	How often there are evaluation exercises based on risks aimed at identifying CIIs and information systems in Senegal. How often the directory of CIIs and information systems in Senegal is updated.	ARTP; ADIE National cyber-security structure	25,000,000
2.1.2 Define the cybersecurity frame-works, procedures and processes required for any institution which owns or manages CIIs and information systems in Senegal	ADIE; National cyber-security structure	Cybersecurity frameworks, procedures and processes required for CIIs and information systems	September 2018	How far are the cybersecurity frameworks, procedures and processes required being applied?	ADIE; National cyber-security structure	25,000,000

2.1.3 Establish a framework for managing the vulnerabilities of government CIIs and information systems to encourage monitoring them regularly	ADIE; CERT/CSIRT	A directory of vulnerabilities, management framework and disclosing vulnerabilities	December 2018	How far is the framework for managing and disclosing vulnerabilities being applied? How often directory of vulnerabilities is updated How often are vulnerability disclosures updated?	ADIE; CERT/CSIRT (national cyber-security structure)	25,000,000
2.1.4 Conduct tests and other regular monitoring activities of Senegal's CIIs and information systems	ADIE; CERT/CSIRT	Tests and other regular monitoring activities of CIIs and information systems	December 2018	How many tests and other monitoring activities are conducted How often tests and other monitoring activities are conducted How effective tests and other monitoring activities are;	ADIE; CERT/CSIRT (national cyber-security structure)	25,000,000
2.1.5 Define minimum security requirements for CIIs and information systems in Senegal.	ADIE CNC National cyber-security structure	Minimum security requirements for CIIs and information systems	December 2019	How far are the minimum security requirements for CIIs and information systems being applied?	ADIE CNC National cyber-security structure	25,000,000

Specific aim 2.2: monitor cyber-threats and manage risks at all times

Expected outcomes

- A coordinated national approach and implementation of incident management have been adopted, supported by a survey of cyber-threats.
- A better understanding of the size and scale of cyber-threats now exists in Senegal since cyber-incidents were reported to the national cybersecurity structure.
- Senegal has a more complete, effective and efficient management of cyber-incidents now there is a central agency for reporting incidents and responses to the national cybersecurity structure.

Strategies/ Actions	Lead and support agencies	Deliverables/ outcomes	Deadline	Key performance indicators	Possible funding sources	Estimated cost (XOF)
2.2.1 Define minimum requirements for keeping incident logs required to analyse them	ADIE; MINT; MFA CERT/ CSIRT	Minimum requirements for keeping incident logs	December 2018	How many entities are adopting and implementing cyber-security incident reporting requirements? Analyse and draw reliable conclusions from cybersecurity incidents	ADIE; MINT: MFA CERT/CSIRT	25,000,000
2.2.2 Monitor, analyse and manage threats and their risks, mitigate, prepare for, respond to and recover from incidents	ADIE; CERT/CSIRT	Measures to mitigate threats and risks and resolve incidents	December 2018	How often are national risk and incident logs updated? How often are measures designed and applied to mitigate and resolve threats and risks?	ADIE; National cyber-security structure	25,000,000

2.2.3 Establish a national register of risks, regulations and directives to promote evaluating and managing risks	ADIE; CERT/CSIRT	National directory of risks, regulations and directives	June 2018	How often is national risk directory updated?	ADIE; National cyber-security structure	25,000,000
2.2.4 Create a log of cyber-incidents, update it constantly, evaluate incidents and propose solutions	ADIE; CERT/CSIRT	Cyber-incident log	September 2018	How often are national risk and incident logs updated? How often are measures to mitigate threats and risks and resolve them developed and applied?	ADIE; CERT/CSIRT	25,000,000
2.2.5 Implement data protection and risk management procedures	CERT/CSIRT	Data protection and management procedures	September 2018	How far are data protection and management procedures being applied?	ADIE; National cyber-security structure	25,000,000
2.2.6 Design and implement cyber-security incident scenarios and simulation programmes to be used in national exercises	CERT/CSIRT	Cyber incident scenarios and simulation programmes	December 2018	Are cyber incident scenarios and simulation programmes being used in exercises on a national scale?	National cyber-security structure	25,000,000

2.2.7 Establish national crisis management measures, test them regularly via cyber-attack exercises and assess the learnings drawn from these exercises to improve these measures	CERT/CSIRT	National crisis management measures	December 2018	How far are national crisis management measures being used?	National cyber-security structure	25,000,000
2.2.8 Create and constantly update an emergency cybersecurity plan describing the roles and responsibilities of the national cybersecurity structure, defence and security forces if there is a cyber-attack	MFA MINT CSIRT	Emergency cyber-security plan	December 2018	How often is the emergency cyber-security plan updated? How effective is the emergency cyber-security plan? How many training exercises are there online?	MFA; National cyber-security structure	25,000,000

Strategic aim 3: promote a cybersecurity culture generally in Senegal

Specific aim 3.1: make all the groups concerned and the public aware of the security risks in cyberspace

Expected outcomes

- Individuals and organisations have adopted good practices so the number, severity and impact of successful cyberattacks which happen in our country can be steadily reduced.
- Individuals and organisations understand how important cybersecurity is, what their responsibilities and obligations are and what they need to do to protect themselves, promoting a cybersecurity culture generally in Senegal

Strategies/ Actions	Lead and support agencies	Deliverables/ results	Deadline	Key performance indicators	Possible funding sources	Estimated cost (XOF)
3.1.1 Conduct a national study to find out how aware of cybersecurity people are at all levels of society and set up a national awareness programme to cover different target groups	MCTPEN CNC National cyber-security structure ANSD	National study of how aware of cybersecurity people are at all levels of society National awareness programme aimed at all user groups, particularly the most vulnerable	September 2018;	Awareness levels How many/ how frequent cybersecurity campaigns are there? How effective are campaigns? How far are national levels of awareness of cybersecurity being evaluated?	MCTPEN CNC National cyber-security structure ANSD	15,000,000

3.1.2 Popularise good practices in cybersecurity	Civil society National cyber-security structure Private sector MCTPEN CNC	National roadmap to inculcate a cyber-security culture in Senegal. Publish/distribute exemplary practices in cybersecurity via multiple communication channels	June 2018;	National roadmap to inculcate a cyber-security culture in Senegal. How often are exemplary practices in cybersecurity published/distributed via multiple communications channels?	Civil society National cyber-security structure Private sector MCTPEN CNC	15,000,000
3.1.3 Provide mandatory cyber-security training for high officials and Board members in private sector so they understand the risks and threats better and how to mitigate them	MCTPEN MESRI MEN CNC National cyber-security structure	Mandatory cyber-security training for high-ranking representatives in government, high-ranking legislators and governance committee members and management of private sector organisations	June 2018;	How much do high officials and Board members in private sector know? How many high officials and Board members are involved in training? How effective is mandatory cyber-security training for high officials and Board members in private sector? How often is there mandatory cyber-security training for high officials and Board members in the private sector?	MCTPEN MESRI MEN CNC National cyber-security structure	20,000,000

Specific aim 3.2: establish an environment of reliable confidence in providing online government services and electronic transactions

Expected outcomes

- Control and minimum cybersecurity requirements are integrated in government services online and electronic transactions, which people and organisations in Senegal or from abroad use in complete confidence

Strategies/ Actions	Lead and support implementation agency	Deliverables/ outcomes	Deadline	Key performance indicators	Possible funding sources	Estimated cost (XOF)
3.2.1 Encourage people to use infra-structure security functions in managing keys and confidentiality, authentication and integrity in particular to create reliable secure environments for government services online and electronic transactions	National cyber-security structure CNC ADIE	Implementation plan for key management infrastructure (KMI)	June 2018;	How many government services online and electronic transactions include using KMI?	National cyber-security structure CNC ADIE ARTP	60,000,000
3.2.2 Migrate from IPv4 to IPv6 protocol	ARTP ADIE National cyber-security structure MCTPEN	Transition plan from IPv4 to IPv6 protocol	December 2018;	How far is the transition plan from IPv4 to IPv6 protocol being applied?	ARTP ADIE National cyber-security structure MCTPEN	50,000,000

3.2.3 Ensure minimum security requirements are paramount in developing government services online and electronic translations to encourage people to trust in digital	National cyber-security structure ADIE All stakeholders involved	Minimum security requirements in developing government services online and electronic transactions	June 2018;	How many government services online and electronic transactions are adopting and using minimum security requirements?	National cyber-security structure ADIE All stakeholders involved	50,000,000

Specific aim 3.3: encourage people to use online government services and electronic transactions

Expected outcome

- People have confidence using government services online and electronic transactions in Senegal

Strategies/ Actions	Lead and support agency (implementation)	Deliverables/ results	Deadline	Key performance indicators	Possible funding sources	Estimated cost (XOF)
3.3.1 Set up national points of contact for cyber-security to collect details of users' concerns about government services online and electronic transactions, respond to these concerns and encourage people to use these services	National cyber-security structure	"Confidence" points of contact	Dec. 2018	To what extent are details of individuals' and organisations' concerns about public and commercial electronic services being gathered and analysed? How confident are individuals and organisations about using public and commercial electronic services?	National cyber-security structure ADIE	50,000,000
3.3.2 Tell the public about cybersecurity measures in place for government services online and electronic transactions	National cyber-security structure ADIE	Programme for sharing details of cybersecurity measures put in place for govern-ment services online and electronic transactions	September 2018	How effectively is information shared? How often do people share information? How much information do they share?	National cyber-security structure ADIE	30,000,000

Strategic aim 4: strengthen resources and technical knowhow in cybersecurity in all sectors

Specific aim 4.1: strengthen resources and technical knowhow in cybersecurity

Expected outcomes

- Senegal will have skills and expertise to monitor, analyser and manage threats and risks constantly and prepare for, mitigate, respond to and recover from incidents

Strategies/ Actions	Lead and support agencies	Deliverables/ results	Deadline	Key performance indicators	Possible sources of funding	Estimated costs (XOF)
4.1.1 Evaluate resources and technical knowhow of national CERT/ CSIRT and govern-ment institutions to deal with weaknesses identified	National cyber-security structure Other stakeholders concerned	Evaluation of resources and technical capacities of national CSIRT and government institutions	December 2018	How many programmes are there are to strengthen weaknesses identified? How often/effective is evaluating resources and technical capacity? How effective are programmes to meet shortcomings and weaknesses?	National cyber-security structure Other stakeholders concerned	25,000,000

4.1.2 Train and guide national CERT/CSIRT staff regularly to face the most sophisticated cyber-threats	CERT/ CSIRT National cyber-security structure	National programme for training CERT/ CSIRT staff	December 2018	Scope of application of national training programme for CERT/CSIRT staff How effective is national programme for training CERT/ CSIRT staff? How many incidents/ attacks/threats/risks have been avoided/ mitigated as a direct consequence of the national training programme for CERT/CSIRT staff?	CERT/CSIRT National cyber-security structure	25,000,000

4.1.3 Train and guide staff of government institutions regularly so they have the skills and knowhow to prepare for, protect against, respond to and recover from incidents.	Stakeholders concerned	Regular training programme for staff of government institutions	December 2018	How far is the national programme for training government staff being applied? How effective is national programme for training government staff? How many incidents/ attacks/threats/risks have been avoided/ mitigated as a direct consequence of the national training programme for government staff?	Stakeholders concerned	10,000,000
4.1.4 Establish basic requirements for cybersecurity training for private and public sectors	MENN MESRI	Basic cybersecurity training requirements	December 2018	How many training programmes there are adopting and implementing basic cybersecurity training requirements?	MEN MESRI	5,000,000

Specific aim 4.2: strengthen resources and technical knowhow required to apply laws and regulations effectively

Expected outcomes

- The organisations responsible for enforcing the law in Senegal have the skills and resources required to tackle cybercrime

Strategies/ Actions	Lead/support agencies	Deliverables/ results	Deadline	Key performance indicators	Possible funding sources	Estimated costs (XOF)
4.2.1 Train and guide security service and judicial authority staff continuously to strengthen their abilities and technical knowhow to tackle cybercrime	MJ MINT MFA MEFP	Training programme for security service and judicial authority staff continuously to strengthen their abilities and technical knowhow to tackle cybercrime	December 2018	How far is the training programme for security service and judicial authority staff being used? How effective is this training programme? How many incidents/ attacks/threats/risks have been avoided/ mitigated through developing the skills and technical knowhow of security service and judicial authority staff?	MJ MINT MFA MEFP	100,000,000

4.2.2 Set up mandatory training in digital investigations and handling evidence for staff of security services, judicial authorities and other organisations working in detecting and prosecuting cybercrime	All stakeholders concerned Gendarmerie/police/ armed forces	Training programme in digital investigation and handling evidence	December 2018	How far is the training programme into digital investigation and handling evidence being applied? How effective is the training programme into digital investigations and handling evidence? How many incidents/ attacks/ threats/risks have been avoided/ mitigated through developing the skills and technical knowhow into digital investigation and handling evidence?	All stakeholders concerned Gendarmerie/police/ armed forces	10,000,000

Specific aim 4.3: ensure good adequate cybersecurity training/jobs

Expected outcomes

- There are national education and training programmes which include cybersecurity at primary, secondary and university level.
- Cybersecurity is recognised as a subject, with admission routes and careers clearly defined.
- Cybersecurity is an essential element of continuing training for all players.

Strategies/ Actions	Lead and support agencies	Deliverables/ results	Deadline	Key performance indicators	Possible funding sources	Estimated cost (XOF)
4.3.1 Draw up a coordinated programme of education and training at national level which includes a secondary and university arm under the auspices of the Ministries concerned;	MEN MESRI	A national programme of cybersecurity education and training	December 2018	How far is the national cybersecurity education and training programme being applied? How effective is the national cyber-security education and training programme?	MEN MESRI	20,000,000
4.3.2 Promote careers in cybersecurity	MEN MESRI MCTPEN	National programme of qualification in cybersecurity	December 2018	Is cybersecurity recognised as a subject with clearly defined admission routes and careers? How far is the national range of cybersecurity subjects being applied?	MEN MESRI MCTPEN	20,000,000

4.3.3 Evaluate and update programmes and documentation for pre-school, primary, secondary and university levels to include cybersecurity ideas	MENMESRI	Programmes and documentation for pre-school, primary, secondary and university levels to include cybersecurity ideas	December 2018	How far are programmes and documentation at pre-school, primary, secondary and university level with cybersecurity ideas being updated? How far are programmes and documentation at pre-school, primary, secondary and university level with cybersecurity ideas being used? How many college graduates are there with the cybersecurity skills required? How effective is updating the programmes and documentation?	MEN MESRI	30,000,000

4.3.4 Draw up partnership agreements between universities and top colleges at home and/or abroad, the public and private sectors to develop study and research programmes and training in cybersecurity	MEN MESRI MCTPEN CNC Universities	New programmes of study and training in cybersecurity Partnerships between government, private sector and academia to handle individuals and organisations being involved in programmes of study, research and training in cybersecurity	December 2018	How many new programmes of study and training are there in cybersecurity? How many students/ graduates are there in new study and training programmes? Scope of involvement in national and international research projects in cybersecurity; How many partnerships have been created to support involvement in national and international research projects into cybersecurity?	MEN MESRI MCTPEN	50,000,000

Specific aim 4.4: promote the growth of the cybersecurity sector in Senegal

Expected outcomes

- Investment in cybersecurity service providers and structures has increased significantly.
- The cybersecurity sector is growing annually, as is its contribution to GDP.
- The Government is supporting local cybersecurity service providers and companies proactively through a range of measures, including public procurement and incentive schemes.

Strategies/ Actions	Lead and support agencies	Deliverables/ results	Deadline	Key performance indicators	Possible funding sources	Estimated cost (XOF)
4.4.1 Promote local and foreign investment in cybersecurity sector in Senegal and offer incentives	MEFP MESRI MPIPDTE MCTEN APIX National cyber-security structure Banks	Programme of incentives to promote investment in cybersecurity	September 2018	How far is the programme of incentives to promote investment in cybersecurity being applied? How effective is the programme of incentives to promote investing in cybersecurity? How many are benefiting from the programme of incentives to promote investing in cybersecurity?	MEFP MESRI APIX Banks National cyber-security structure	60,000,000

4.4.2 Conduct studies into how cybercrime is affecting Senegal's economy.	National cyber-security structure	Study results published on how cybercrime is affecting Senegal's economy	June 2019	How often are studies on how cybercrime is affecting Senegal's economy updated? How much is being invested in cyber-security thanks to the study results?	National cyber-security structure	25,000,000
4.4.3 Support local businesses which specialise in developing and providing cybersecurity solutions	MEFP MESRI APIX MCTPEN Banks National cyber-security structure	Funding and incentive programme for local businesses which specialise in developing and providing cyber-security solutions	September 2018	How many businesses are involved in the funding and incentive programme for local businesses? How effective is the funding and incentive programme for local businesses? Scope of application of funding and incentive programme for local businesses	MEFP MESRI APIX Banks MCTPEN	80,000,000

Strategic aim 5: be involved in regional and international cybersecurity work

Specific aim 5.1: strengthen bilateral and multilateral collaboration on cybersecurity issues

Expected outcomes

- Senegal is involved actively and effectively in regional and international cybersecurity work.
- There is more bilateral and multilateral collaboration on cybersecurity issues.

Strategies/ Actions	Lead and support agencies	Deliverables/results	Deadline	Key performance indicators	Possible funding sources	Estimated cost (XOF)
5.1.1 Coordinate Senegal's involvement and collaborate more with other States and regional and international partners on cybersecurity, particularly in fighting cybercrime	SGPR MAESE National cybersecurity structure MCTPEN ARTP	Programme to coordinate and involve Senegal and its collaboration with other States and regional and international partners on cybersecurity, particularly in fighting cybercrime Agreements and partnerships signed with partners on cybersecurity and fighting cybercrime	September 2018	How far has the programme to coordinate and involve Senegal and its collaboration with other States and regional and international partners been implemented? How effective is the programme to coordinate and involve Senegal and its collaboration with other States and regional partners? How far have the appropriate frameworks been implemented? How effectively have the appropriate frameworks been implemented? How often is information on potential threats shared via international links or networks? How many potential attacks from information from international links or networks?	SGPR MAESE National cyber-security structure MCTPEN ARTP	5,000,000

5.1.2 Be actively involved in regional and international cyber-security activities, particularly fighting cybercrime	GEN SEC PRESIDENT'S OFFICE MAESE National cybersecurity structure MCTPEN MINT MJ MFA ARTP	Plan of regional and international involve-ment in cybersecurity in fighting cybercrime Funds to participate more actively in cyber-security activities and fighting cybercrime Participate in key international forums on cybersecurity and fighting cybercrime. Publish results/lessons learned from being involved in regional and international activities in cyber-security and fighting cybercrime	September 2018	How far has the regional and international plan on cybersecurity and fighting cybercrime been implemented? How far have the funds to be involved more actively in cybersecurity activities and fighting cybercrime been used? How far are we involved in key international forums on cybersecurity and fighting cybercrime? How effectively have results/lessons learned been drawn from being involved in international and regional activities in cybersecurity and fighting cybercrime?	GEN SEC PRESI-DENT'S OFFICE MAESE National cyber-security structure MCTPEN MINT MJ MFA ARTP	15,000,000

8 ANNEXE B – PRIORITY PROJECTS

Estimated costs and deadlines see Annexe A.

Strategic aim 1: strengthen the legal and institutional framework of cybersecurity in Senegal
1. **Establish and implement national cybersecurity structure for Senegal** 2. Strengthen legal cybersecurity structure
Strategic aim 2: strengthen protection of critical information infrastructures (CIIs) and government information systems in Senegal
3. Project to identify and protect critical information infrastructures (CIIs)
Strategic aim 3: promote a cybersecurity culture in Senegal
4. Produce a national roadmap for promoting a cybersecurity structure in Senegal 5. Establish a national awareness programme aimed at all user groups, particularly the most vulnerable. 6. Cybersecurity training programme for government authorities, other institutions in the Republic and Board members of public and private sector organisations.
Strategic aim 4: strengthen cybersecurity abilities and technical knowhow in all sectors
7. Training and reinforcement programme for national cybersecurity resources 8. Minimum rules and standards for training and education in cybersecurity 9. National coordination programme of education in cybersecurity and skills development 10. National incentive scheme to promote investment in cybersecurity
Strategic aim 5: be involved in regional and international cybersecurity work
11. Plan of regional and international involvement in cybersecurity, particularly in combating cybercrime 12. Establish a national fund to take part actively in cybersecurity activities, particularly in fighting cybercrime.

9 ANNEXE C – GLOSSARY

- Authentication: for an IT system, authentication is a process which enables that system to verify that a request for access made by an entity (human being or some other system) is legitimate so it can allow that entity to access the system's resources (systems, networks, applications) in accordance with the access control parameters.

- Confidentiality: ensuring data can only be accessed by those authorised to do so

- Cyberattack: a malevolent act on an IT resource via a cybernetic network

- Cybercrime: breaches of international treaties or national laws, using information systems or networks as means of committing crimes or targeted at them.

- Cybersecurity: a set of security laws, policies, tools, devices, concepts and mechanisms, risk management, action and training methods, good practices and technologies which can be used to protect IT people and assets connected directly or indirectly to a network of states or organisations to keep them available, integrated and authentic, confidential, proven and non-repudiated).

- Cyberspace: cyberspace is the global environment in which information and communication systems are interconnected. Cyberspace is larger than the IT world, and also includes IT networks, IT systems, digital media and data, whether real or virtual.

- Distributed denial of service (DDoS): a kind of attack which renders a service unavailable to its normal users, disturbing the normal operation of the system by making large numbers of requests.

- Phishing is an insidious system used to get you to reveal your personal details, such as passwords or credit card, social security or bank account numbers.

- Cyber incident: an event which represents a potential or actual threat to a device, computer or network connected to the Internet and/or data processed, stored or transmitted on this data and which may need to be responded to to mitigate the effects.

- Social engineering: manipulating people psychologically for the purposes of fraud. Social engineering uses psychological, social and, more widely, organisational weaknesses to get something from its intended victims (goods, services, bank transfers, physical or IT access, disclosing confidential information etc.)

- Integrity: a system's integrity is the means by which an IT system is protected against malfunctions, aggression and attacks.

- Internet: the global public access IT network, a network of networks, with no central brain, made up of millions of networks, both public and private, academic, commercial and governmental, grouped in autonomous networks themselves.

- The Internet of things: a global infrastructure for the information society which can be used to use advanced services by interconnecting objects (physical or virtual) thanks to interoperable information and communication technologies which exist or are evolving.

- Malware: any kind of software which seeks to harm an IT system without the user's consent. Malware includes viruses, worms, trojans and other threats.

- Cyberthreats: anything which can compromise security or damage devices, computers, software or networks online, all the data they contain and the services they provide or support.

- Non-repudiation: being able to verify that the sender and receiver are in fact the parties who sent or received a message.

- Ransomware: a kind of malware which takes personal data hostage, by encrypting it then demanding that their owner sends money in exchange for the key which can be used to decrypt it. Ransomware can also prevent users accessing a machine until a key or release tool is sent to the victim in exchange for a sum of money.

- Resilience: an information system's ability to resist a breakdown or cyberattack and restore itself after an incident.

- Risks: the effects of data being attacked without attacking the information system and/or the effects of attacking an information system.

- Vulnerability: a weakness in an IT system which enables an attacker to undermine that system's integrity, that is, its normal workings, or the confidentiality or integrity of the data which it contains.