Cybersecurity Capacity Review of the Republic of Senegal

Global Cyber Security Capacity Centre
University of Oxford
22/2/2016

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Contents

List of Abbreviations

ADIE	Agency for the State Information Technology
ARTP	Regulatory Agency for Telecommunications and Posts
CDP	Commission for the Protection of Personal Data
CIRT	Computer Incident Response Team
CNI	Critical National Infrastructure
CMM	Cybersecurity Capacity Maturity Model
CSIRT	Computer Security Incident Response Team
ECOWAS	Economic Community Of West African States
ESMT	Ecole Supérieure Multinationale des Télécommunications
GCSCC	Global Cyber Security Capacity Centre
GFCE	Global Forum on Cyber Expertise
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
GoTa	Global open Trunking architecture
ICT	Information and communications technology
ISP	Internet Service Providers
IT	Information technology
ITU	International Telecommunications Union
MEFP	Ministry of Economy, Finance and Planning
MOI	Ministry of Interior and Public Security
MPT	Ministry of Post and Telecommunications
SGG	Secretary General of the Presidency
SME	Small and medium-sized enterprises
UVS	Université Virtuelle du Sénégal

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Cybersecurity Capacity Review of the Republic of Senegal

Introduction

Through collaboration with the Dutch Government under the auspices of the Global Forum on Cyber Expertise (GFCE), the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity maturity in the Republic of Senegal, supported by the national host team from the Ministry of Post and Telecommunications. The objective of this exercise is to enable the government to prioritise areas of capacity in which the country might strategically seek invest in order to improve their national cybersecurity posture.

During January (19th - 21st) 2016, stakeholders from the following sectors participated in a four-day consultation to review the cybersecurity capacity in the Republic of Senegal:

- Public Sector Entities:
    - Secretariat of the President of the Republic;
    - General Secretariat of the Government (Office of the Prime Minister);
    - National Assembly;
    - Ministry of Posts and Telecommunications;
    - Ministry of Interior and Public Security;
    - Ministry of the Armed Forces;
    - Ministry of Economy, Finance and Planning (MEFP);
    - Regulatory Authority for Telecommunications and Post (ARTP);
    - Commission for the Protection of Personal Data (CDP);
    - Agency for the State Information Technology (ADIE);
    - National Agency of Statistics and Demography (ANSD);
    - Regulatory Authority for Public Procurement (ARMP);
    - Directorate for the Promotion of Digital Economy and Partnerships (DPENP);
    - Operational Office for Monitoring the 'Emerging Senegal Plan' (BOSSE);
    - The Economic, Social and Environmental Council;
    - Ministry of Health and Social Action;
    - Ministry of Agriculture and Rural Equipment;
    - Ministry of Women, Family and Children;
    - Ministry of Environment and Sustainable Development;
    - Ministry of Livestock and Animal Production;
    - Ministry of Local Governance, Development and Spatial Planning;
    - Ministry of Labour, Social Dialogue, Professional Organizations and Institutional Relations;
    - Ministry of Youth, Employment and Citizen Building;
    - Ministry of Public Service, the Rationalization of the Workforce and the Public Sector Renewal;
    - Ministry of Sports;
    - Ministry of Higher Education and Research;
    - Ministry of Education;
    - Ministry of Infrastructure, Land Transport and Opening;
    - Ministry of Industry and Mines;

  - Ministry of Trade, Informal Sector, Consumer Affairs, Promotion of Local Products and SMEs;
  - Ministry of Investment Promotion, Partnerships and the Development of TV Services of the State;
  - Ministry of Energy and Renewable Energy Development;
  - Ministry of Tourism and Air Transport;
  - Ministry of Vocational Learning and Crafts;
  - Ministry of Culture and Communication.
- Legislators/Policy owners
- Criminal Justice and Law Enforcement
- Armed forces
- Academia
- Civil Society
- Private Sector
- Telecommunications companies
- Finance sector
- Cyber Task Force
- Contact points for the Global Forum on Cyber Expertise (GFCE)
- Regional and international organisations

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model (CMM)[1] which is composed of five distinct dimensions of cybersecurity capacity:

1) Policy and strategy;
2) Culture and society;
3) Education, training and skills;
4) Legal and regulatory frameworks;
5) Standards, organisations, and technologies.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. Table I below shows the five dimensions with their comprising factors:

Table I: Description of Factors within Each Dimension

Dimension	Factors in Each Dimension
Dimension 1 Cybersecurity Policy and Strategy	D1-1: Documented or Official National Cybersecurity Strategy
	D1-2: Incident Response
	D1-3: Critical National Infrastructure (CNI) Protection
	D1-4: Crisis Management
	D1-5: Cyber Defence Consideration
	D1-6: Digital Redundancy
Dimension 2	D2-1: Cybersecurity Mind-set
	D2-2: Cybersecurity Awareness

[1] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

Cyber Culture and Society	D2-3: Confidence and Trust on the Internet
	D2-4: Privacy Online
Dimension 3 Cybersecurity Education, Training and Skills	D3-1: National Availability of Cyber Education and Training
	D3-2: National Development of Cyber Security Education
	D3-3: Training and Educational Initiatives within the Public and Private Sector
	D3-4: Corporate Governance, Knowledge and Standards
Dimension 4 Legal and Regulatory Frameworks	D4-1: Cybersecurity Legal Frameworks
	D4-2: Legal Investigation
	D4-3: Responsible Reporting
Dimension 5 Standards, organisations, and technologies	D5-1: Adherence to Standards
	D5-2: National Infrastructure Resilience
	D5-3: Cybersecurity Marketplace

In each factor there are indicators spanning five stages of maturity. Here the start-up stage implies an ad hoc approach to capacity and ranges up to the dynamic stage where a strategic approach and the ability to dynamically adapt or change against environmental considerations is included. The five stages are as follows:

- **Start-up:** At this stage, there is either no cybersecurity maturity, or it is embryonic in nature. Initial discussions about cybersecurity capacity building might be in place, but no concrete actions have been taken. There is an absence of observable evidence at this stage.
- **Formative:** Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply "new". However, evidence of this activity can be clearly demonstrated.
- **Established:** The elements of the sub-factor are in place, and working. There is not, however, well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the "relative" investment in the various elements of the sub-factor. However, the indicator is functional and defined.
- **Strategic:** Choices have been made about which parts of the indicator are important, and which are less important for the particular organisation or nation. The strategic stage reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances.
- **Dynamic:** Clear mechanisms are in place to alter strategy, depending on the prevailing circumstances such as the technology of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride, in a "sense-

and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

This report presents the results following the cybersecurity capacity review of the Republic of Senegal and includes recommendations on the next steps to be considered in order to increase the cybersecurity capacity maturity of the country.

Executive Summary: Cybersecurity Capacity Review of the Republic of Senegal

The Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') has facilitated a review of the maturity of cybersecurity capacity of the Republic of Senegal, hosted by the Ministry of Post and Telecommunications of Senegal. The objective of this review is to enable the Republic of Senegal to gain the understanding of its cybersecurity capacity necessary to prioritise investment strategically in cybersecurity capacities.

During January (19th, 20th and 21st) 2016, stakeholders from the following sectors participated in several consultations over three-day: government departments and ministries, academia, civil society, legislators and policy owners, Information Technology leaders from government and the private sector, major industry, telecommunication companies and the financial sector. The consultations were premised on the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five distinct areas of cybersecurity capacity:

- Policy and strategy
- Culture and society
- Education, training and skills
- Legal and regulatory frameworks
- Standards, business models and technologies

Policy and Strategy

Through roundtable consultations, the *policy and strategy* dimension of cybersecurity capacity for the Republic of Senegal was identified to range from *start-up* to *formative stages* of maturity. Senegal does not have a national cybersecurity strategy document. However, the Cyber Task Force, which was consolidated by the Ministry of Post and Telecommunications (MPT), brings together key stakeholder groups and has started to discuss the development of a national cybersecurity strategy.

No national CSIRT or command and control centre structure exists, which poses a challenge to effective and coordinated incident response and management. No regulation that requires incidents to be reported is in place and Senegal lacks a mandated authority or protocol to handle such a process.

The government has not established a central list of CNI assets. As a consequence, communication between the government and CNI operators is ad-hoc and coordination is limited, whether general or cyber-specific. In cases where a coordinated response would be required, neither a cybersecurity operational strategy or plan, nor an official mandate is in place to manage and mitigate cybersecurity incidents. Similarly, risk management exercises or cyber drills are not conducted at a national level.

Regarding crisis management considerations, no official planning and evaluation of crisis management protocols and procedures currently takes place. No mandate for risk management planning has been assigned and the Republic of Senegal does not have a specific defence policy or strategy. While the army and gendarmerie have specialised cyber defence

structures in place, there is no strategic coordination or command and control structure for cybersecurity.

Various redundancy efforts within the private sector are in place, including the creation of continuity plans in the event of a crisis. However, the dissemination of such plans, as well as the coordination of efforts between the public and private sectors is currently lacking.

Culture and Society

During consultations the national capacity considered in the *cybersecurity culture and society* dimension was identified to range between *start-up* and *formative* stages. At a governmental level, cybersecurity was identified as a concern, but it was noted that IT experts across government departments are usually the ones most aware of cybersecurity, while general awareness is comparatively low. The majority of employees and high-level officials do not have the same threat awareness and understanding as IT staff. Some large organisations in the private sector, such as telecommunications operators and banks, possess a good understanding of cybersecurity threats and risks and are therefore found to place priority on building a cybersecurity mind-set by identifying high-risk practices. However, small and medium-sized enterprises were found not to possess the same understanding of the need for cybersecurity. Society-at-large is seen to have very limited awareness of cyber threats. In addition, there is no coordinated awareness-raising programme or campaign at a national level to cover all groups in society and with defined targets and goals. Moreover, promotion of safety online at a national level is lacking.

Some e-government services in Senegal have been developed, but uptake is low and there is currently no coordinated effort to secure and promote trust in these services. Similarly, the use of online banking services and e-commerce services is still low. Initiatives to promote trust in the use of online services are generally lacking and, consequently, the knowledge of users regarding safe online practices is limited. This has led to an environment where users either 'blindly' use the Internet or are discouraged from using online services because of a general distrust. Comprehensive legislation on privacy has been adopted, but implementation is limited. The recognition of privacy as an important component of cybersecurity in the workplace is increasing, but still considerably low.

Education, Training and Skills

Through the consultation, it was observed that the *cybersecurity education, training and skills* capacity in Senegal is at a *formative stage*. At the university level, there are limited educational offerings available in information security and cryptography, but not specifically in cybersecurity. Education on information and communications technology (ICT) and related security issues has not yet penetrated into the curriculum of all levels of education. Similarly, no nationally coordinated cybersecurity education and training programme has yet been established.

Academic and private sector actors have started to develop and offer some targeted cybersecurity training and certifications, but these remain ad-hoc and uncoordinated. Cybersecurity training programmes for employees in the private sector are equally limited and mainly focused on IT staff. Within some organisations, higher executive levels of senior

management (C-level management) are found to have an understanding of cybersecurity issues, but not of how these might affect the organisation or what direct threats organisations may face. Board directors rely on their IT departments for guidance on cybersecurity, which reduces the priority placed on cybersecurity investments.

Legal and Regulatory Frameworks

During the consultations *legal and regulatory frameworks* were identified to range between *start-up* and *established* stages of maturity. In 2008 Senegal adopted a wide range of laws that address cybersecurity. The *Law No. 2008-10 on Orientation Law on Information Society,* the *Law No. 2008-08 on Electronic Transactions* and *the Law No. 2008-41 on Cryptology* build a framework for national ICT security and this is intended to ensure secure e-commerce, e-transaction and cryptology services. Data protection and online privacy is provided for by the *Law No. 2008-12 on the Protection of Personal Data*, which is enforced through the Commission for the Protection of Personal Data (CDP). Finally, substantive and procedural aspects of cybercrime are covered by the *Law No. 2008-11 on Cybercrime.* However, the implementation of this legal framework varies and is generally not sufficient. Since 2008, none of the laws have been amended to reflect the changing environment of cybersecurity.

Law enforcement has some capacity to investigate computer-related crimes, in particular through a specialised brigade against cybercrime. Adequate specialised training, however, is not widely available for all law enforcement officers, which limits investigative capabilities. Prosecutors and judges are not trained adequately and do not have the capacity to prosecute and preside over computer-related crimes. Furthermore, no national policy or framework on responsible disclosure exists.

Standards, Business Models and Technologies

The Senegalese capacity in *cybersecurity standards, business models and technologies* was identified to range from *start-up* to *formative* stages. Cybersecurity standards have been identified for use and some standards, such as ISO/IEC 27001 are adhered to within some parts of public and private sectors. However, different departments within the government and organisations adhere to different standards according to their needs, customer demands and requirements imposed by international parent and partner organisations, rather than government regulations. Currently, standards implemented in procurement and software development practices do not yet fully meet international IT guidelines, standards and acceptable practices.

Internet services infrastructure is increasingly reliable, leading to the growing use of the Internet for varied purposes. National infrastructure resilience is managed primarily by ARTP, but coordination with the private sector is still low. The cybersecurity marketplace is underdeveloped and foreign technologies are being deployed instead of producing security products domestically. Furthermore, the need for developing a cybercrime insurance market was not yet identified at a national level.

Additional Reflections

This was the eleventh country review that we have supported directly, and the first conducted as an initiative of the Global Forum on Cyber Expertise (GFCE). We hope that this review will

offer useful insights to the Republic of Senegal and that our recommendations on how to increase cybersecurity capacity will contribute to the development of a National Cybersecurity Strategy.

The Global Cyber Security Capacity Centre

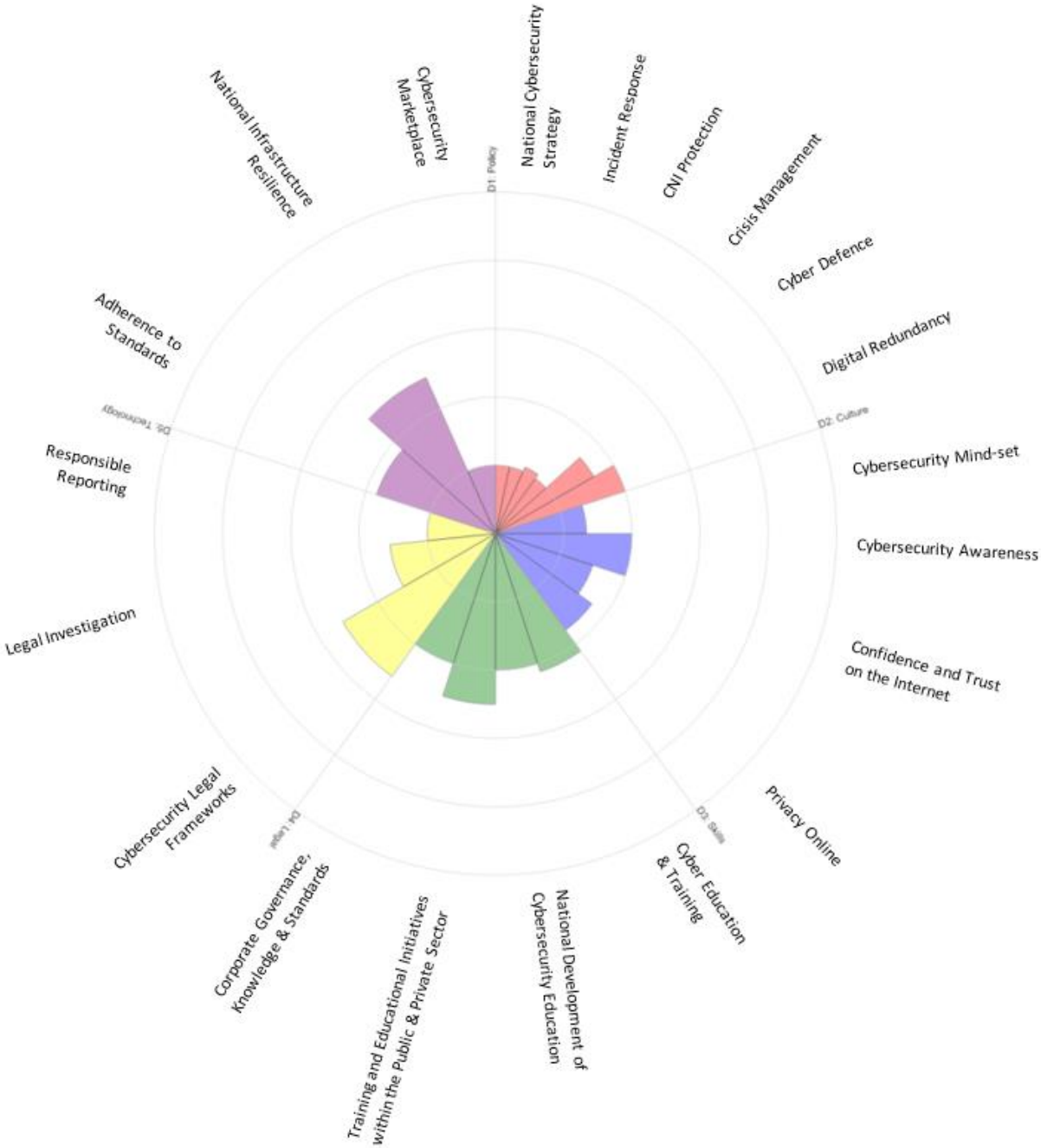
Review of Cybersecurity Capacity Maturity

In this section, we provide an overall presentation of the cybersecurity capacity in the Republic of Senegal. The graphic facing (Graphic I), presents the maturity estimates in each dimension. The stages of maturity for each factor extend out from the middle as an individual bar, and each dimension is a fifth of the graphic.

As seen in this graphic, the collected evidence shows that for most factors the cybersecurity capacity in the Republic of Senegal lies between a *start-up* and *formative* stage of maturity. Only some elements of one factor within Dimension 4 (Legal and regulatory frameworks) does maturity appear to be moving towards an *established* stage. However, according to the methodology followed during the application of the Cybersecurity Capacity Maturity Model (CMM), all the indicators for a certain stage need to be achieved for that stage of maturity to be assigned. Otherwise, maturity is recognised only at the highest completed stage. The assignment of maturity stages is based upon our interpretation of the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and our professional judgement.

Table I (see Appendix) presents a summary of the results on the stage of maturity for each factor, including a brief description of those results. Links to key policy and strategy documents, laws and other additional information are provided in the Table. Table II (Appendix) presents a total of sixty-nine recommendations regarding the enhancement of the existing capacity for each factor.

Graphic I: Review Results



Dimension 1: Cybersecurity Policy and Strategy

Not every government has established a national level cybersecurity policy and strategy, or a body responsible for policy and strategic implementation. Cybersecurity as a policy area is still evolving. However, the importance of designating an overarching government body for cybersecurity coordination and having a national cybersecurity strategy and policy is very important. International experience shows that those governments that have taken these measures are much better placed to address and mitigate cyber-incidents and attacks. This dimension explores the capacity of the government to design, produce, coordinate and implement a cybersecurity strategy.

D1-1: Documented or Official National Cybersecurity Strategy

Cybersecurity policies and strategy are an essential part of efforts to mainstream a cybersecurity agenda within government and a state. The Implementation of policies and the creation of a strategy helps indicate where and how cybersecurity is to be prioritised. To this effect, it helps to determine areas of responsibility and mandates of key cybersecurity government actors. Further, it helps to indicate direct allocation of resources to the emerging and existing cybersecurity issues and areas to prioritise.

Stage: Start-up

At this point, there is no official national cybersecurity strategy document in Senegal which would serve as a coordinative document for the various existing ad-hoc initiatives. However, proactive efforts are underway to begin the process of developing such a national strategy, chiefly the congregation of a Cyber Task Force comprised of members of varying ministries, private-sector actors, academia, and civil society with a stake in cybersecurity.[2] While this group has only met twice since its formation in early 2015, such a multi-stakeholder group is a critical component for successful strategy development.

There are several agencies, ministries and organisations that conduct ad-hoc cybersecurity initiatives. The Ministry of Post and Telecommunications (MPT) has led in the consolidation of Cyber Task Force members and has helped drive momentum for recognition of the need for a cybersecurity strategy, while the Agency for the State Information Technology (ADIE) is tasked with the implementation of information technology (IT) policy in the country.[3] Several participants suggested that ADIE's responsibility extends to the implementation of cybersecurity as well. Other central organisations to be considered when developing a national strategy include: the National Commission of Cryptology, Army, Gendarmerie, Regulatory Agency for Telecommunications and Posts (ARTP), Commission for the Protection of Personal Data (CDP), and the Secretary General of the Presidency (SGG), among others. Given the abundance of organisations and efforts made in the area of cybersecurity, a central

[2] Members of the Task Force inter alia include representatives of the Ministry of Post and Telecommunications (MPT), Department of Justice, Agency for the State Information Technology (ARTP), Regulatory Agency for Telecommunications and Posts (ARTP), Commission for the Protection of Personal Data (CDP), Cheikh Anta Diop University, National Army, Gendarmerie, Article 19, and SENTRUST.
[3] http://worldloop.org/projects/adie-dakar-senegal/

organisation responsible for cybersecurity was widely regarded as critical by all participants in the review.

Such a central organisation could be either a newly established organisation or an existing organisation that receives a mandate for coordinating cybersecurity nationally. Participants felt that national coordination is currently lacking and that the creation of a national cybersecurity strategy that determines clear roles and responsibilities is of great importance. On the other hand, some participants believed there should be agreement at the conceptual level regarding what cybersecurity consists of and how it differs from cybercrime notions. If such convergence on conceptualization of cybersecurity is incorporated into strategy development, then the identification of roles and responsibilities will be clearer.

D1-2: Incident Response

This factor speaks to the capacity of the government to identify and determine characteristics of national-level incidents, events or threats in a systematic way – preferably, through a central registry. It also reviews the government's capacity to organise and coordinate an incident response.

Stage: Start-up

Currently, there is no national incident response organisation that would serve as the coordinating body for the reporting and management of cybersecurity incidents in the country. Such organisations mostly take the form of Computer Security Incident Response Teams (CSIRT) or Computer Incident Response Teams (CIRT). Due to the lack of a central organisation, there is no single entity holding a central registry of national level incidents. If a consumer wants to report an incident, the individual would usually contact the operators or consumer protection agency, rather than a body specifically tasked with incident response. In 2011 ITU IMPACT conducted a CIRT assessment in order to determine the readiness of the country to implement a national CIRT, and has commenced engagement to plan the establishment of a national CIRT.[4]

However, while there is no central incident response body yet, there is nevertheless some incident response capacity. For example, within the Ministry of Economy and Finance (MEFP), a project through which internal information systems are audited on an annual basis was established in 2007 and revised in 2011 (*Audit de la Sécurité du Système d'Information du Ministère de l'Economie et des Finances*).[5] Participants indicated that the audit, conducted through the Ministry's Directorate for Automatic Processing of Information (DTAI), resulted in the development of a security paper on this system, which in turn led to the strengthening of the information security and incident response capability specifically within the General Directorate of Customs, which is subordinated to the MEFP. In addition, there is a cybercrime brigade within the National Police Directorate which has both the digital forensics and

[4] http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf
[5] http://www.dtai.finances.gouv.sn/assimef.php

technical laboratory capacities to assist in investigation, but this does not encompass incident response responsibilities.

Finally, although there is no coordination mechanism for incident response at the national level, in 2014, ARTP instigated a telephone traffic monitoring and antifraud project in Senegal, which aimed at enhancing control and transparency of the telecommunications sector and to reduce the financial losses due to telecom fraud.[6] Within this project, ARTP is working with the Gendarmerie to arrest perpetrators of online fraud. Additionally, a recent Prime Minister's decree aims to establish a national centre for cybercrime, which could serve as a coordinative body that would help facilitate incident response. However, so far these initiatives remain ad-hoc and only loosely related to incident response. In order to truly address this issue, an organisation with the mandate to solely focus on incident response would be important to elevate maturity in this factor.

D1-3: Critical National Infrastructure (CNI) Protection

This factor studies the government's capacity to identify CNI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CNI asset owners, and enable comprehensive general risk management practice including CNI risk management.

Stage: Start-up

No official list of what kind of industries and companies comprise critical national infrastructure has been created, although most participants felt that there was a common understanding of what such a list would consist of. During the review, several participants listed a number of organisations or sectors that would represent CNI, including telecommunications, water, energy (including electricity supply systems), oil and fuel, police networks, and others. ADIE was considered to be particularly important for securing the telecommunications infrastructure and was referenced several times during the discussions of this factor. Nonetheless, there is no single ministry or network of ministries responsible for the coordination of critical infrastructure in relation to cybersecurity. Participants highlighted that *Law No. 2008-12 on the Protection of Personal Data* does not require infrastructure operators to report and share information on cybersecurity incidents, such as data or system breaches, which was perceived as a shortcoming of the law. Similarly, although *Law No. 2008-08 on the Electronic Transactions* sets some requirements for Internet Service Providers (ISPs) regarding the reporting of illegal content, participants stated that the implementation of these provisions of the law are insufficient. Moreover, there is no requirement for ISPs to manage or report illegal activities on their networks.

While response planning is not handled in a formally coordinated and structured manner, at the operational level, first responders and engineers will often work through the Global open

[6] http://www.globalvoicegroup.com/en/news/item/19-control-of-international-call-volumes-in-senegal

Trunking architecture (GoTa) Network in order to collaborate after cybersecurity incidents have occurred, including with foreign counterparts.

As regards coordination across CNI operators, no formal communication channels or collaboration mechanisms have been established. However, participants from the banking, electricity, and transportation industry referred to the ORSEC plan (Le Plan national d'organisation des secours), which is a general national emergency plan that lays out procedures and roles and responsibilities in case of disaster.[7] The plan provides a basis for national emergency risk management, which is coordinated by the High Commission of Civil Protection (CSCP) and the Directorate of Civil Protection (DPC).[8] Although the plan is not specific to cyber incidents, but covers any type of national disaster, it could serve as the foundation for the development of a CNI coordination mechanism and risk management procedures that are specific to cybersecurity.

Similarly to national risk management, internal risk management practices within CNI have not yet been extended to cybersecurity. While some examples of non-cyber risk management were cited, such as recent efforts of the Ministry of Interior and Public Security (MOI) to enhance disaster and risk management, the overall perception confirmed that cybersecurity is not yet on the radar of many infrastructure providers when analysing organisational risks.

D1-4: Crisis Management

Crisis management planning and evaluation capacity, bolstered by functional protocols and standards, is critical to implementing cybersecurity policies that are results-oriented and sustainable. Crisis management planning usually entails but is not limited to conduct of specialized needs assessments, training exercises, and simulations that produce useful results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would underpin recommendations for policymakers and other stakeholders and inform national strategy implementation as well as budgetary allocations.

Stage: Start-up

Very little was said about cybersecurity crisis management efforts, other than that exercises and simulations are not conducted at the national level in Senegal. According to some of the government stakeholders, crisis management is sometimes conducted at the organisational level or within ministries and agencies, but these measures are ad-hoc and vary depending on the organisation. Details about these organisational crisis management efforts were not discussed in the review.

[7] http://www.servicepublic.gouv.sn/assets/textes/orsec.pdf
[8] https://acasis.locean-ipsl.upmc.fr/lib/exe/fetch.php?media=yanon_revue_critique_des_plans_de_contingences_au_se_ne_gal.pdf

D1-5: Cyber Defence Consideration

This factor explores whether the government has the capacity to design and implement a cyber defence strategy and lead its implementation including through a designated cyber-defence organisation within the executive branch. Among other considerations, it also reviews the level of coordination between various public and private sector actors in response to malicious attacks on military information systems and critical national infrastructure.

Stage: Start-up – Formative

Cyber Defence capacity maturity in Senegal ranges between *start-up* and *formative*, depending on the indicators observed. In terms of Cyber Defence strategy, there is no overarching strategy or policy that would provide a framework for managing cyber defence at the national level. Within the Army and Gendarmerie, separate initiatives and approaches addressing cybersecurity have been formulated, but participants indicated that the national defence strategy and conventional defence approaches are applicable to cyber-attacks. Hence, a defence strategy that would be specific to cyberspace was not considered necessary. There have been discussions about the role of cyberspace as a domain of warfare, but no official documentation has been developed in order to cement this into practice. A consolidated national approach towards cyber defence strategy or policy would ensure that relevant stakeholders in the army and gendarmerie operate in a coordinated fashion and that defence measures take into account the specific challenges posed by cyber-attacks.

On the other hand, organisational capacity to manage cyber defence is closer to the *formative* stage of maturity. Both the Gendarmerie and the National Police have dedicated units for cybercrime and cyber defence, which have a key role in cyber defence management, receive similar training and report to the same government ministries. There is a regular exchange of expertise between the police and military units, which facilitates continuous coordination between the two. In practice, virtual and physical security is not sufficiently executed across the military, and coordination is lacking between other national level organisations and defence organisations.

D1-6: Digital Redundancy

Digital redundancy foresees a cybersecurity system in which failure of any component is safeguarded against by fall-back services. Most of these services will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network). This factor reviews government's capacity to plan and organize redundancy communications among stakeholders.

Stage: Formative

There was a sharp divergence of views between government participants and defence participants in the review regarding the maturity of digital redundancy efforts. According to government representatives, mainstream operators that manage digital systems do have redundancy systems in place. While these redundancy networks are not interlinked, each

network operator takes issues of digital redundancy into consideration and continuity plans are in place. Redundancy mechanisms extend not only to physical network redundancy, but also to management efforts.

However, the management element of redundancy was not reflected by the defence participants. They considered the lack of connectivity and coordination between people in different services as a gap in digital redundancy. ADRASEC,[9] a lesser-known private organisation of radio services that works in crisis and disaster management, was referenced as to its potential as a valuable resource in ensuring that redundancy efforts, roles and responsibilities are effectively communicated to all relevant parties. ADIE's management of network resilience, as well as MEFP's management of local networks will also be important for unifying digital redundancy efforts. Participants noted, however, that effective digital redundancy requires substantial financial resources, which are scarce in Senegal.

Data-backup is currently mainly conducted through external contractors, which poses a security risk.

Recommendations

Following the information presented from the review of the maturity of *Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Senegal. These recommendations aim to provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided separately for each factor.

Official National Cybersecurity Strategy

For the Republic of Senegal to make progress on cybersecurity, the key issue to address is the lack of an overarching entity for cybersecurity coordination. With no official national cybersecurity strategy and no central body overseeing cybersecurity activities in Senegal, responsibility is scattered across different departments. The establishment of the Cyber Task Force has been an essential first step towards developing such a strategy, with multi-stakeholder collaboration as a continued key component. The following recommendations have been outlined for consideration:

- R1-1: Embark toward developing a National Cybersecurity Strategy to set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. This strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives.
- R1-2: Allocate a specific mandate for the implementation of the National Cybersecurity Strategy.
- R1-3: Design and disseminate a coordinated cyber programme.

[9] http://www.senrasec.org/

- R1-4: Strengthen and promote inter-departmental cooperation in cybersecurity.

Incident Response

Without a national CSIRT or other central incident response body, there will be no effective way to share information and resolve incidents at the national level. Communication channels between actors remain ad-hoc and inconsistent in incident response, impeding effective incident management. Therefore, the following recommendations have been outlined for consideration:

- R1-5: Categorise and record national-level cyber incidents in a central registry.
- R1-6: Work towards the development of a national CSIRT with clear processes and defined roles and responsibilities.
- R1-7: Draft legislation, which allocates mandates to the national CSIRT.
- R1-8: Develop a coordination and information sharing mechanism between the private and the public sector.
- R1-9: Appoint and publicize a national-level lead to ensure reporting of incidents and promote reporting.
- R1-10: Define lines and channels of communication for crisis situations within the government.

Critical National Infrastructure (CNI) protection

No central list of CNI assets has been identified by government. There is no defined cybersecurity operational strategy or plan in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber-attack on CNI. Incident response by CNI is also uncoordinated, without a formal cyber response plan or official mandate. Risk management exercises and drills are not conducted at a national level. Therefore, the following recommendations have been outlined for consideration:

- R1-11: Develop a national list of Critical National Infrastructure (CNI) assets with identified risk based priorities.
- R1-12: Establish a mechanism for regular vulnerability disclosure and information sharing between the public and private sector.
- R1-13: Establish information protection and risk management procedures and processes, supported by adequate technical security solutions, which inform the development of an incident response plan.
- R1-14: Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CNI operators.
- R1-15: Allocate budget for conducting emergency response scenario exercises.

Crisis management

No official planning and evaluation of crisis management protocols and procedures are in place. Equally, there is no mandate for risk management planning. Therefore, the following recommendations have been outlined for consideration:

- R1-16: Conduct a needs assessment of measures that require testing with consideration of a simple exercise scenario.
- R1-17: Allocate a mandate for planning of exercises.
- R1-18: Include all stakeholders in the planning and evaluation of the exercises.
- R1-19: Conduct compromised communication scenarios and exercises to test emergency response assets interoperability and function effectively.
- R1-20: Evaluate the exercises and feed the findings back into the decision-making process.

Cyber Defence Consideration

There is no defence policy or strategy for cyber defence considerations. The various efforts of the Army and Gendarmerie are conducted on an ad-hoc basis but there is no strategic coordination between these efforts, nor external engagement outside of the task force. Therefore, the following recommendations have been outlined for consideration:

- R1-21: Commence the development of a Cyber Defence Strategy which takes into consideration identified threats to national security in cyberspace.
- R1-22: Develop a central command and control centre or structure for cyber defence.
- R1-23: Enhance coordination in response to malicious attacks on military information systems and critical national infrastructure.
- R1-24: Conduct consistent review of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.

Digital redundancy planning

Various redundancy efforts in Senegal are to be commended, particularly with the creation of continuity plans in the event of a crisis. However, the dissemination of such plans, as well as the coordination of efforts between the public and private sectors is currently lacking. Therefore, the following recommendations have been outlined for consideration:

- R1-25: Allocate appropriate resources to not just hardware integration, technology stress testing, personnel training and crisis simulation drills, but also on ensuring redundancy efforts are appropriately communicated.
- R1-26: Hardwire all emergency response assets into a national emergency communication network.
- R1-27: Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.

Dimension 2: Cyber Culture and Society

Even the most forward-thinking cybersecurity strategies and policies are of little help if a wide array of actors are not formally charged with implementing cybersecurity or actors do not understand their roles and responsibilities as users and stakeholders in safeguarding sensitive and personal data as they use digital media and resources. This dimension reviews important elements of a responsible cyber culture and society at the individual and organisational level as perceived by a variety of stakeholders. Aspects of a secure cyber culture include the level of trust users have in Internet services, such as in e-government and e-commerce, and the adherence to standards of privacy in handling personal information by all the entities that engage in provision of these services. This dimension underscores the centrality of users in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programs for users – systems they can use easily and incorporate in their everyday practices online.

D2-1: Cybersecurity Mind-set

This factor evaluates the level of recognition and priority attached to cybersecurity in the values, attitudes, and practices of government, the private sector, and society-at-large to demonstrate a cybersecurity mind-set. A cybersecurity mind-set is understood as a predisposition and, in certain cases, as a consistent, routinized behavioural pattern in aligning one's actions with good cybersecurity priorities both at an individual level and in an organisational setting. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-up – Formative

When reviewing the cybersecurity mind-set within Senegal, the review looked at three groups of actors: government, private sector, and society-at-large. The perception of government mind-set toward cybersecurity was that technical staff is aware of the need for cybersecurity, but this attitude does not extend to wider contexts within government institutions. The creation of the Cyber Task Force discussed above was viewed as one mechanism for raising the awareness of cybersecurity among non-technical staff. Civil society participants were of the opinion that certain cybersecurity issues, like hacking or illegal content, are engrained into the government's mind-set, but that there is no broad understanding of cybersecurity. Academic participants, however, believed that the lack of implementation of cybersecurity laws and policies is indicative of a lack of mind-set. The lack of a broader awareness campaign promoted by the government was also cited as evidence for an underdeveloped mind-set.

Academic and civil society participants also partially disagreed regarding their perception of the private sector's mind-set. Those from academia believed that the cybersecurity mind-set of the private sector is similar to that of the public sector. There are some leading banks and e-commerce entrepreneurs that are more aware than other private sector actors, but these organisations represent the minority. Civil society participants, on the other hand, felt that

the private sector even lags behind the public sector and academia in awareness of cybersecurity. They also expressed that government bodies should put pressure on the private sector to recognise the need for cybersecurity and data protection.

Across society-at-large, a cybersecurity mind-set is emerging among selected groups, in particular academia and civil society organisations. As the country becomes more digitised, more students are trained in and exposed to cybersecurity, which is raising a cybersecurity mind-set among the academic community. Likewise, civil society organisations are proactive in promoting a cybersecurity mind-set. However, there is not yet an engrained cybersecurity mind-set across society. This is partially due to a lack of awareness raising efforts and partially because Internet access is still limited in some regions of Senegal.

D2-2: Cybersecurity Awareness

This factor presents the need for programs to raise cybersecurity awareness with special emphasis on the perception of cyber-risks and threats. Awareness raising programmes need to cover a wide range of target groups of society and their effectiveness should be observed and measured.

Stage: Formative

The need for awareness of cybersecurity threats and vulnerabilities has started to be recognised, although national cybersecurity awareness raising campaigns have not yet been established. Some civil society actors have started to put efforts into targeted cybersecurity awareness-raising, and participants agreed that a 'common ground' between government, private sector and civil society could enable the proliferation of awareness raising to the broader society. The government needs to work alongside existing efforts in academia to ensure that new initiatives capitalise from the academic experience. Such synergy is critical to ensure that awareness-raising efforts are efficient and effective.

Several structures were referenced regarding their potential to serve as platforms for building awareness raising campaigns. For instance, ADIE or the association of IT professionals might function as drivers in promoting cybersecurity awareness. In addition, a network of education professionals has started to analyse international experiences in this area, which could be helpful in the development of a national awareness raising campaign. In this context, a best practice guide is being developed for cybersecurity awareness, but a national programme through which such practices would be adopted and implemented is still lacking.

D2-3: Confidence and Trust on the Internet

This factor reviews the level of stakeholders' trust in the use of online services, in general, and e-government and e-commerce services, in particular. Users need to be aware of cybersecurity risks, but not become so fearful that they avoid using valuable online services.

Stage: Start-up – Formative

During the review, there was general agreement among participants that trust in the secure provision of online services highly relates to the level of cybersecurity awareness in the country. Some examples of a lack of trust in online services were provided by participants. In particular, academic participants had doubts as to whether the security of univerities' online enrolment services are trustworthy. As a result of this distrust, the University of Dakar has not yet fully implemented this service. Other examples include distrust of online payment mechanisms due to experiences involving inadequate security.

The relationship between the lack of cybersecurity awareness and trust in service provision presents itself in relation to data protection. Most citizens are unaware of how their personal data might be used by online service providers, which can either lead to blind trust or unwarranted distrust in service provision. In addition to a lack of awareness, participants expressed doubts about the security of government websites, as there have been some hacking incidents related to these sites, even though reportedly no sensitive data were leaked.

The state of e-government and e-commerce services is currently embryonic. ADIE has established an online platform, which allows citizens to access various administrative services, including tax returns.[10] One participant raised the issue that there can be no bargaining for tax payments if done online, which is a common practice in offline transactions. Hence, many citizens prefer to use paper-based options for their taxes. The development of e-government services has also been a long process, which is undermining citizens' trust in these services. Finally, the range of available e-commerce services is still very limited. E-banking services are still very new to Senegal and most payments are done in cash.

D2-4: Privacy Online

This factor reviews the level of salience of issues concerning the protection of personal data as illustrated by the government agenda through enactment of relevant practices, laws, and regulations, and the level of engagement and advocacy around them by civil society. It also evaluates how national legislative norms adhere to regionally and internationally recognised standards for human rights.

Stage: Start-up - Formative

In the context of privacy and data protection, Senegal has taken concrete steps to increase the maturity of its capacity to the *formative* stage. *Law No. 2008-12 on the Protection of Personal Data*, as well as the establishment of the Commission for the Protection of Personal Data (CDP), which is inter alia meant to keep close watch on the mass collection of personal data, represent significant steps towards improved privacy and data protection. Several participants felt that the right to be forgotten would be considered a positive aspect of new legislation, but has not yet been adopted into legislation. Cases were cited in which spyware was used at the workplace by employers to monitor and expose employees. However, cases

[10] http://servicepublic.gouv.sn/.

were brought against these employers and they were prosecuted for their actions. The data protection law states that employers must disclose the fact that they deploy surveillance measures, which seeks to safeguard certain privacy rights.

The reason why Senegal has not yet fully reached the *formative* stage of cybersecurity maturity within this factor is the insufficient application of the *Law No. 2008-12 on the Protection of Personal Data*. Participants claimed that the corporate culture in public and private sectors is intrusive in nature and a delineation of the boundaries of employers and their responsibilities as regards data protection is needed. Communicating the duty of employers to protect both employee data and their privacy is needed in order to elevate the maturity of this factor to the next stage.

Recommendations

Based on these consultations, the following recommendations are provided for consideration by the government of Senegal regarding the maturity of *cyber culture and society*. These aim to provide advice and next steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model.

Cybersecurity Mind-set

Cybersecurity is not yet a priority across all levels of the government, however IT experts across government are seen to have more knowledge and understanding of cybersecurity. The general majority of employees and high-level officials do not have the same understanding of cybersecurity. Some companies within the telecommunication sector and banks have an understanding of cybersecurity threats and risks, and place priority on building a cybersecurity mind-set by identifying high-risk practices. Most companies are however found not to recognise the same need for cybersecurity. Society at-large has some awareness of cyber threats, particularly within academia and civil society. However, a cybersecurity mind-set is adopted inconsistently and not engrained across society. To promote a cybersecurity mind-set within all sectors it is recommended to:

- R2-1: Enhance efforts at all levels of government to promote understanding of risks and threats, but also to design systems that enable users across society to more easily embed secure practices into their everyday use of the Internet and online services.
- R2-2: Work on promoting sharing of information on incidents and best practices among organisations to promote a proactive cybersecurity mind-set.
- R2-3: Promote prioritisation of risk and threat understanding for private sector entities by identifying high-risk practices.
- R2-4: Develop programmes and materials to train the public and improve cybersecurity practices.

Cybersecurity awareness

There is no coordinated programme or campaign at a national level in Senegal that covers all groups in society with defined targets and goals and no advertisements or promotion of safety online at a national level. To enhance the existing capacity it is recommended to:

- R2-5: Develop a national awareness raising programme to cover various target groups, focusing on the most vulnerable users.
- R2-6: Link the development of the programme to the process of the national cybersecurity strategy development.
- R2-7: Engage multiple stakeholders in the development and delivery of the awareness raising programme.

Confidence and trust on the Internet

Trust in online services is identified as a concern. Users do not have enough knowledge regarding safe online practises and the Internet is often used with "blind" trust or distrust. Online banking services are still underdeveloped, the use of e-commerce is limited, and e-government services are largely under development. In order to enhance the level of trust in secure online services we suggest the following actions:

- R2-8: Expand e-government services with recognition of the need for the application of security measures to promote trust in e-services.
- R2-9: Promote adherence to cybersecurity protection standards for e-government services.
- R2-10: Promote the need for security in e-commerce services.

Privacy Online

The importance of privacy is understood at the governmental level and laws on personal data protection exist, but impact is lacking due to insufficient application. Moreover, there is minimal understanding of the importance of privacy in the workplace among private sector leaders. Therefore, the following actions are recommended:

- R2-11: Promote understanding and initiate discussions regarding the implementation of privacy standards and policies within government.
- R2-12: Sensitise private sector leaders and employees on employee privacy rights and obligations.

Dimension 3: Cybersecurity Education, Training and Skills

This dimension reviews the availability and quality of cybersecurity education, training, and skills in Senegal for various groups of government stakeholders, private sector, and the population as a whole. In particular, it evaluates existing educational offerings and national development of cybersecurity education; training and educational initiatives within public and private sector; and corporate governance, knowledge, and standards.

D3-1: National Availability of Cybersecurity Education and Training

This factor speaks to the importance of availability of high quality cybersecurity education and training options, their integration and synergies, in order to ensure adequate and sustainable supply of cybersecurity skills for the needs of public and private sectors. It takes stock of existing educational offerings in schools and universities and training offerings within private sector and beyond it in the field of information security and cybersecurity and provides a superficial evaluation of their structure and components.

Stage: Formative

The availability of cybersecurity education and training in Senegal varies depending on the demographic in question. Efforts are underway within the education system to establish advanced cybersecurity programmes. At Cheikh Anta Diop University (University of Dakar), several post-graduate courses within the Department of Mathematics and Computer Science are available, such as the research and professional Master programmes in Data Transmission and Cryptography and the Doctorate in Coding, Cryptography, and Algebraic Applications.[11] These degrees all have information security components either as mandatory components or electives. At the African Center of Excellence in Mathematics, Computer Science and ICT (CEA-MITIC) at the Université Gaston Berger - Saint-Louis, new courses are being created which contain information security components, such as a Master's in Cryptology, Coding and Applications, and a Master's in Secure Embedded Systems in Mobile.[12] Finally, while the University of Bambey does not have official degrees in security related fields, it does have certification offerings in security systems and software.[13] However, there are no official cybersecurity courses offered. Below the university level, no official cybersecurity education has been established by academic institutions.

A range of training programmes are offered either through universities or other organisations, such as the Senegalese Internet Society (ISOC), which holds cybersecurity awareness raising training for children. Most trainings, however, focus on ICT professionals, including network administrator training and professional certifications offered by Ecole Supérieure Multinationale des Télécommunications (ESMT). Such certifications include Certified Secure Computer User (CSCU) and others through the virtual university Université Virtuelle du

[11] http://edmi.ucad.sn/index.php?option=com_content&view=article&id=22&Itemid=27.
[12] http://www.ceamitic.sn/index.php.
[13] http://www.uadb.edu.sn/index.php/les-formations-en-tic.

Sénégal (UVS).[14] ADIE is offering training programmes, but lacks strategic deployment. Occasionally, there are tailored trainings from universities and technical organisations that are developed ad-hoc, following specific requests. Participants of the review raised the urgent need for more professional trainings, as well as more training for non-professionals, for instance through mandatory orientation courses for new employees. Some participants expressed concerns regarding the general lack of awareness of the need for centralised training centres and standardised training programmes. If demand for training provision was higher, then training centres might be more readily established.

D3-2: National Development of Cyber Security Education

This factor explores what kind of structure exists for the national development of cybersecurity education: for example, whether any education strategy for developing cybersecurity skills exists; whether cybersecurity as a discipline is given priority in educational curricula; whether adequate budget allocation is present.

Stage: Formative

Many participants felt that a national programme for promoting cybersecurity education and training within the Ministry of Education would be important for enhancing capacity, but such a programme has not yet been developed. As a consequence, some participants felt that inadequate efforts are being made both by the government and academia. Some participants criticised the government for not offering enough financial or political support for enhancing cybersecurity capacities in universities, while others felt that the universities are too inflexible in the provision of courses. Including cybersecurity education in the development of the national cybersecurity strategy could help resolve some of these issues.

Due to the prolific ad-hoc programmes and certifications that have been developed in academia to enhance internal capacity, Senegal has reached the formative stage within this factor. More coordination at the national level and the establishment of a national education and training programme would increase the maturity of this factor.

D3-3: Training and Educational Initiatives within the Public and Private Sector

Cybersecurity is a highly technical specialized field, and therefore strategic development and deployment of skillsets and tools to support them is central to keeping organisations secure and mainstreaming cybersecurity culture within organisational structures. Apart from the question of strategic staffing, this factor assesses the scope of horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates to continuous skills development.

[14] http://www.uvs.sn/.

Stage: Formative

There was disagreement among some participants regarding the extent of cybersecurity knowledge transfer between employees. The perception of civil society is that, in private companies, there is a knowledge management skill deficiency. Staff responsible for developing skills and training, lack cybersecurity understanding, which adversely affects the broadening of the cybersecurity skillset across the nation. Some participants proposed to enhance training initiatives, such as by developing a guidance document for raising the awareness and skills across the workforce, or providing more advanced professional cybersecurity courses that include a knowledge-transfer component.

Other stakeholder groups, such as criminal justice and CNI, claimed that efforts are being made within various organisations to share knowledge and skills gained in cybersecurity trainings. The Ministry of Trade, Informal Sector, Consumer Affairs, Promotion of Local Products and SMEs cited specific examples of its IT staff receiving supplementary training on cybersecurity, which was then shared with broader staff. New, wider training initiatives have targeted criminal justice employees, which includes knowledge sharing. However, most participants agreed that the sharing of cybersecurity knowledge and skills has not been institutionalised into training offerings and induction courses for new employees within organisations.

D3-4: Corporate Governance, Knowledge and Standards

This factor specifically looks into how private and state-owned companies, as represented by the highest executive level of senior management (C-level management), understand cybersecurity and react to changes related to the cybersecurity status quo.

Stage: Formative

Board-level understanding of cybersecurity varies across different organisations in Senegal, and is primarily limited to general risks rather than cyber-specific risks. Senior decision-makers within academia do not yet consider cybersecurity risks and in the private sector, cybersecurity is still primarily viewed as an IT issue rather than a strategic board-level concern. Even within some critical infrastructure sectors, such as water and electricity, participants felt that cybersecurity is not yet considered to be a major risk, even though processes are becoming increasingly tied to automated information systems. Managers of small and medium-sized enterprises (SME), which represent a significant percentage of the private sector in Senegal, do not yet consider cybersecurity as a concern in business operations.

On the other hand, some organisations, such as ARTP and banks, are beginning to incorporate cybersecurity into their strategic decision-making at the board-level. The Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) is working with Senegalese banks on this issue, including through the provision of internal trainings through specialised training departments, utilising foreign expertise, sharing information internationally, and

shifting accountability for cyber incidents to management rather than solely IT staff. The West African Central Bank is also finalising a new regulation, which seeks to fully recognize cybersecurity in risk and security management procedures across the banking sector.

Recommendations

Following the information presented on the review of the maturity of cybersecurity education, training and skills, the following set of recommendations are provided to the government of Senegal. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model.

National Availability of Cybersecurity Education and Training

In Senegal, educational offerings are available in information security and cryptography, but not specifically in cybersecurity. There are some laboratories that have been set up that may play a key role in furthering cybersecurity education in Senegal. Training in information security is ad-hoc and training courses, seminars and online resources are limited. In order to enhance the level of capacity regarding the national availability of cybersecurity education and training, we recommend the following actions:

- R3-1: Engrain cybersecurity training and education throughout all levels of education.
- R3-2: Allocate additional resources to cybersecurity education and training for public universities.
- R3-3: Identify training needs and develop training courses, seminars and online resources for targeted demographics, such as users and experts.
- R3-4: Create cybersecurity career opportunities and promote the attractiveness of cybersecurity careers to wider leadership roles.

National Development of Cyber Security Education

While there are some offerings in cybersecurity education in Senegal, there is no national programme that seeks to promote efforts at a wider, strategic level. Until now, there is no coordinated funding for cybersecurity research and cooperation between academia and the government should be enhanced. Regarding the development of cybersecurity education, we recommend the following actions:

- R3-5: Develop a nationally coordinated programme on cybersecurity education and skills development.
- R3-6: Allocate budget for training and research and development in cybersecurity, and start multi-stakeholder discussions on how to promote cybersecurity as a 'profession' with clear career pathways.
- R3-7: Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy.

- R3-8: Create obligatory cybersecurity modules for students and teachers in order to promote knowledge in cybersecurity and create an interest for careers in cybersecurity.

Training and Educational Initiatives within the Public and Private Sector

Cybersecurity training programmes for employees are not consistent across Senegal and mainly directed on IT staff. The following recommendations are proposed to enhance the capacity of training and educational initiatives:

- R3-9: Establish basic requirements for cybersecurity training for the public and private sectors.
- R3-10: Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.
- R3-11: Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms.

Corporate Governance, Knowledge and Standards

Senior management in selected sectors has an understanding of cybersecurity issues, but not of how these might affect the organisation in detail or what direct threats they might face. It is common for boards to rely on IT departments. To improve the corporate governance, knowledge and standards for cybersecurity the following actions are recommended:

- R3-12: Conduct mandatory cybersecurity trainings for board members to enhance the understanding of the overall organisational business risk from cyber threats, in a regular manner.
- R3-13: Promote cooperation and communication channels between technicians and CEO's to transfer the need for investment in cybersecurity.

Dimension 4: Legal and Regulatory Frameworks

International experience attests to the crucial role legal and regulatory frameworks play in mainstreaming cybersecurity across sectors while presenting prevention, mitigation, and dispute mechanisms to individuals and organisations affected by cyber-threats. This dimension looks into the government's capacity to develop and enact national legislation and accompanying by-laws directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, cybercrime, and on the stakeholder groups represented by law enforcement, prosecution services, and courts. It also evaluates how national legislative norms adhere to regionally and internationally recognised standards for human rights.

D4-1: Cybersecurity Legal Frameworks

This factor reviews the availability and comprehensiveness of ICT security and privacy and data protection legislation, its relation to human rights legislation, as well as a country's status in relation to regional and international treaties directly or indirectly related to cybersecurity.

Stage: Formative – Established

The maturity of cybersecurity capacity within legal frameworks in Senegal varies across the different types of laws and their implementation. While not all participants were aware of the full scope of legislation addressing cybersecurity, Senegal has adopted a wide range of applicable laws in 2008. In particular, four relevant laws were references by participants: *Law No. 2008-08 on Electronic Transactions*, *Law No. 2008-11 on Cybercrime*, *Law No. 2008-12 on the Protection of Personal Data* and *Law No. 2008-41 on Cryptology*. In addition, Senegal passed *Law No. 2008-10 on Orientation Law on Information Society*, which inter alia lays out general principles regarding the security of the 'information society', as well as privacy, protection of data and other human rights.

ICT security is mainly covered in two laws. Firstly, *Law No. 2008-08 on Electronic Transactions* aims at providing a legal framework for the safe emergence of a reliable e-commerce sector in Senegal, sets rules and procedures for Internet Service Providers, and supports the development of electronic transactions and contracts by specifying the requirements for electronic evidence and signatures. Secondly, *Law No. 2008-41 on Cryptology* defines the terms and conditions of the use, supply, import and export of cryptology means and services.

As regards privacy, data protection and other human rights, *Law No. 2008-12 on the Protection of Personal Data* was highlighted by participants as the most advanced in terms of implementation. Both the private and the public sector are involved in the application of the law. Moreover, in order to ensure effective enforcement of the provisions, the government established the Commission for the Protection of Personal Data (CDP). The main obstacle of full implementation of the law is monitoring its application at the provincial, city, town and village levels. Some participants from the criminal justice system reported that law

enforcement does not receive sufficient training to fully understand and comply with the various components of the law.

Apart from the Data Protection Law, the privacy of communications is protected under Article 13 of the Constitution of Senegal. Senegal has also signed and ratified the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Both substantive and procedural provisions on cybercrime are addressed in *Law No. 2008-11 on Cybercrime*, which was built on the *Criminal Code of Senegal (Law N° 65/60 of 21 July 1965*) and the *Criminal Procedure Code of Senegal* (*Law N° 65/61 of 21 July 1965*) to reflect the new elements of the cyberspace dimension. Some participants of the criminal justice system criticised that the law is not flexible enough to be effectively implemented. In addition, defence participants pointed out that the law partially refers to the Criminal Code and Criminal Procedure Code, which are not up-to-date anymore. In relation to cross-border cooperation on cybercrime, various available channels are utilised, in particular through the national INTERPOL office. However, dual criminality was raised as an impediment of effective collaboration.

Senegal has also started the process of accession to the *Budapest Convention* and has implemented the *Economic Community of West African States (ECOWAS) Directive on Fighting Cyber Crime* in its Criminal Code. Ratification of the *African Union Convention on Cybersecurity and Personal Data Protection* has not yet commenced.

Despite the establishment of a comprehensive legal framework, participants noted that the highly dynamic cybersecurity sector is not reflected in these laws, which have not been amended or adapted since 2008. As a consequence, some laws show redundancies and overlaps, which should be addressed through legal revision. In 2008, the ICT and cybersecurity sector in Senegal was not yet fully developed, hence a clear vision of legal requirements was not yet possible. An amendment of the laws would ensure that they reflect the current realities and challenges of cybersecurity. Furthermore, while every possible measure is taken to ensure that the principle of technology neutrality is enforced and laws cover a broad range of issues, participants criticised that the laws are currently not sufficiently enforced, as comprehensive mechanisms for the implementation are lacking.

D4-2: Legal Investigation

This factor studies the capacity of executive branch of government to prevent, combat, and investigate cyber incidents, attacks, and crimes, and of judiciary branch to prosecute cybercrime and electronic evidence cases. It also looks into the dynamic of formal and informal collaboration between different branches of government and between government and court system.

Stage: Start-up – Formative

Among the actors involved in the investigation and prosecution of cybercrime, law enforcement has the highest level of capacity. A specialised brigade on cybercrime (Brigade spéciale de lutte contre la cybercriminalité) within the police was established under the EU Global Action on Cybercrime project (GLACY) and is working routinely with network and information system managers. Some digital forensics capabilities exist that ensure that data remain unaltered in the investigations. In addition, ARTP has the necessary resources to assist investigations on a regular basis.

The cybercrime brigade also receives basic training. However, criminal justice participants stated that current training is not sufficient and should be more specialised and practical to reflect the realities of cybercrime investigations. As a consequence, law enforcement capacities remain limited, despite being the most advanced capacity in cybercrime investigation and prosecution. Similarly, international collaboration is performed on an ad-hoc basis rather than being engrained in daily practices.

In contrast to law enforcement, participants were of the view that magistrates are not skilled to handle cybercrime cases, which has inter alia led to long custody durations for cybercrime perpetrators. Specialised cybercrime prosecutors are not yet in place. Although first training programmes have been conducted for prosecutors, these are not institutionalised. For instance, in the framework of the GLACY project, experts have trained magistrates in cybercrime. While this project has enabled criminal justice officials from Senegal to engage actively with international counterparts, participants noted that this cooperation is limited as Senegal has not yet ratified the Budapest Convention.

Similarly to prosecutors, the capacity of courts to handle cybercrime cases was perceived as low. Judges also do not receive training to understand the expert opinions in cybercrime cases.

D4-3: Responsible Reporting

This factor explores if the public and private sectors enact a responsible disclosure policy and if there is sufficient capacity on part of both to continuously review and update this policy and synchronise it with recognised international responsible disclosure mechanisms. It also analyses existing capacity of stakeholders to receive, analyse, and disseminate vulnerability information gleaned through the responsible disclosure mechanisms.

Stage: Start-up

No official responsible disclosure mechanism has been established in Senegal to receive and disseminate vulnerability information. Defence participants of the review suggested that, once a national CSIRT has been established, that body could initiate the development of a national responsible disclosure framework. An issue that was raised is the reluctance of private sector companies to disclose vulnerabilities because of credibility concerns.

On an informal level, ADIE is screening telecom networks for vulnerabilities. In one case, ADIE informed MEPA of an outdated content management system (CMS) used for the ministry's website. As a result, the ministry updated the CMS.

More progress was achieved regarding consumer reporting in the telecommunications industry through a consumer complaints platform. After consumer complaints have been received, cases are forwarded to courts or are addressed with operators directly.

Recommendations

Based on the review of the maturity of legal and regulatory frameworks the Centre has developed the following set of recommendations to be considered by the government for the enhancement of existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model.

Cybersecurity Legal Frameworks

In 2008, comprehensive ICT security legislation and regulatory frameworks have been established in Senegal. *Law No. 2008-10 on Orientation Law on Information Society, Law No. 2008-08 on Electronic Transactions* and *Law No. 2008-41 on Cryptology* have laid the foundation to ensure a safe online environment, secure online transactions, e-commerce and the regulated use of cryptology services. Data protection was addressed in *Law No. 2008-12 on the Protection of Personal Data* and substantive and procedural cybercrime provisions are contained in *Law No. 2008-11 on Cybercrime.* However, the implementation of the laws has been limited and fragmented, and the legal framework has not been amended to ensure applicability to the current state of cybersecurity in Senegal. Therefore, in order the maturity to progress at a higher stage, we recommend the following:

- R4-1: Review and amend existing laws on cybersecurity, data protection and cybercrime to address gaps and overlaps.
- R4-2: Fully ratify and implement regional and national cybercrime instruments, including through the allocation of sufficient resources according to national priorities.
- R4-3: Review and improve legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime.

Legal Investigation

Law enforcement is considered to have some capacity to investigate cybercrime in accordance with domestic law, however this is minimal. Prosecutors and courts are not trained adequately and do not have the capacity to prosecute and preside over cybercrime cases. In order to enhance legal investigation capacity we recommend the following:

- R4-4: Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.
- R4-5: Develop and institutionalise specialised training programmes for police, prosecutors and judges in computer related crime.
- R4-6: Establish and strengthen formal and informal international cooperation mechanisms within the police and criminal justice system.

Responsible Reporting

No official national policy or framework is in place for responsible reporting of vulnerabilities. Regarding issue, we recommend the following:

- R4-7: Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledgement report.
- R4-8: Encourage sharing of technical details of vulnerabilities among CNI.

Dimension 5: Standards, organisations, and technologies

This dimension explores the importance of implementation of cybersecurity standards and at least minimal acceptable practices; existence of well-functioning and high-capacity organisations coordinating cybersecurity with formal authority over multiple stakeholders; and existence of a vibrant cybersecurity marketplace of technologies and cyber-insurance services.

D5-1: Adherence to Standards

This factor reviews the government's capacity to design or adapt from other jurisdictions and implement cybersecurity standards and at least minimal acceptable practices, especially those related to procurement procedures and software development. These standards and practices provide a minimum necessary baseline in the context of which strategic government decisions, especially organisational (resource) and financial (budgetary), should take place.

Stage: Start-up – Formative

Within the adherence to cybersecurity standards, most sectors have reached the formative stage of maturity, but the adoption of security standards within procurement is impeding progression in this factor. ADIE is leading the efforts to promote the incorporation of more security standards into practice in Senegal. ADIE has started to develop a specific in-house project on cybersecurity standards, which has not yet been fully implemented, but has instigated discussion on strategic issues. This includes work on developing security standards for interoperable and interconnected networks. Some government organisations and IT firms have adopted ISO27001, which is intended to feed into an overall government security risk assessment in the future. However, apart from these specific examples, the adoption of cybersecurity standards in Senegal is mainly driven by requirements imposed by multinational parent companies. For example, the Senegalese banking sector has adopted international security standards related to international payment systems (EMV standards through VISA). However, although some standards have been adopted, they are largely not mandated or recommended by government ministries or organisation (apart from the mentioned efforts by ADIE).

Within procurement standardisation, the code of public procurement is aiming to ensure transparency and accountability, but does not address cybersecurity requirements. As a result, most participants stated that the strategic focus of procurement is primarily focusing on function and price rather than security aspects. This is a significant gap in the adoption of security standards to enhance cybersecurity.

The adoption of cybersecurity standards within software development is at early stages in Senegal. The telecommunications operators Orange, Sonatel and Tigo have started to implement software procurement standards due to increasing consumer demands. Meanwhile, banking applications are mandated to to abide by some security standards, but this does not apply to other sectors. Similarly to procurement standards, software

development cybersecurity standards need to be developed and proliferated to key institutions in order to enhance maturity in this capacity.

D5-2: National Infrastructure Resilience

This factor explores how effectively the government deploys and manages infrastructure technologies and how it performs monitoring and evaluation of the costs for infrastructure technologies and their resilience. In addition, it looks into existence and exercise of government's capacity to engage in strategic planning and maintain sufficient scientific, technical, industrial, and human capabilities.

Stage: Formative

Participants considered the resilience of the telecommunications infrastructure in Senegal to be more advanced than other regional counterparts. ADIE, while it does not provide the technical support for telecommunications, helps to ensure that the provisions of Internet service is resilient. There was disagreement among some participants about the degree of resilience of ISPs, some claiming that there are shortcomings and weaknesses in service provision, while others claimed that interconnected platforms external to Senegal are the source of such weaknesses. Through the already mentioned telephone traffic monitoring and antifraud project, ARTP is hoping to solve some of these regional issues in cooperation with its neighbouring counterparts and regionally operating organisations, such as ITU and ECOWAS. Energy supply remains a problem in Senegal, as well as low internet penetration (approximately 29%). As penetration expands, resilience will become an increasingly important issue.

While ARTP and ADIE lead resilience efforts nationally, there is a perceived lack of coordination between the public and private sectors regarding governing resilience efforts. Improving this coordination would be a positive step to increasing capacity within this factor.

D5-3: Cybersecurity Marketplace

This factor studies the availability of competitive cybersecurity technologies and their strategic deployment and maintenance by public and private sectors. It also reviews the state cyber-insurance marketplace and its offerings through the study of perception of financial risks by public and private sectors and perceived demand for cybercrime insurance.

Stage: Start-up

At the time of the review, a cybersecurity market has not yet fully developed, because general awareness of cybersecurity issues is still too low. Stakeholders were not aware of any domestically produced cybersecurity products. Research and development efforts are still low, but there is an increasing interest within academia to engage in constructive efforts to stimulate growth of the cybersecurity market.

Similarly, a cybercrime insurance market has not yet begun to develop. One private sector representative was concerned that evaluation of insurance policies is many times more than the technology is actually worth. Overall, the cybercrime insurance market as a whole is still inadequate in Senegal.

Recommendations

Based on the review of the maturity of standards, organisations, and technologies, the following recommendations are provided to be considered by the government of Senegal. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model.

Adherence to Standards

Information security standards have been identified for use, with ISO/IEC 27001 standards adhered to within selected areas of the public and private sectors. However, standards are not promulgated widely and different departments within the government and organisations adhere to different standards according to their needs. Procurement and software development security standards are not yet widely adopted. Therefore, the following actions are recommended:

- R5-1: Establish a programme to strengthen government's capacity to adapt or adopt international standards in order to acquire a baseline in the context of organisational cybersecurity.
- R5-2: Promote adoption of international IT standards, in particular during procurement, software and code development.
- R5-3: Promote the awareness and implementation of standards among SME.

National infrastructure Resilience

Internet services infrastructure is increasingly reliable, leading to the growing use of the Internet among Senegalese society for varied purposes. National infrastructure resilience is managed primarily by ARTP, but coordination with the private sector is still low. The following recommendations are provided to increase the maturity of national infrastructure resilience:

- R5-4: Increase reliability of online government services and promote their full deployment.
- R5-5: Develop a national programme for infrastructure development.
- R5-6: Work on enhancing the level of security processes in place (threat assessments and risk management processes).
- R5-7: Invest in ICT research and cooperation between academia, research and industry to strengthen the software-engineering competencies of domestic ICT companies.

Cybersecurity Marketplace

Technologies are not produced domestically, but imported. Regarding cybercrime insurance, there is a perspective that the regional development of insurance offerings is not a viable option at this point. Therefore, we recommend:

- R5-8: Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development.
- R5-9: Promote sharing of information and best practices among organisations, to continue to explore potential cybercrime insurance coverages.

Appendix

Table I: Review Results

Dimension	Capacity Factor	Stage of Maturity	Brief Description	References
Dimension 1 Cyber Security Policy and Strategy	**D1-1 National Cybersecurity Strategy**	**Start-up**	The drafting of a national cybersecurity strategy has not yet commenced. With no official national cybersecurity strategy and no central body overseeing cybersecurity activities in Senegal, responsibility is scattered across different departments. The Ministry of Post and Telecommunications has consolidated a Task Force that brings together key national stakeholders in cybersecurity.	
	D1-2 Incident Response	**Start-up**	There is no national CSIRT and no command and control centre. Communication channels between actors remain reactive, ad-hoc and inconsistent in incident response, impeding effective incident management.	ITU IMPACT http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf Audit of the Security of the Information System of the Ministry of Economy and Finance http://www.dtai.finances.gouv.sn/assimef.php
	D1-3 Critical National Infrastructure	**Start-up**	No central list of CNI assets has been identified by government. Interaction between government ministries and owners of critical assets on cybersecurity is limited. A cybersecurity operational strategy or plan to manage and mitigate cybersecurity incidents in case of a coordinated cyber-attack on CNI is not in place. Incident response by CNI is uncoordinated, without a formal cyber response plan or official mandate. Risk management exercises and drills specific to cybersecurity are not conducted at a national level.	Decree No. 93-1288 of 17 November 1993, adopting the National ORSEC Plan http://www.rag.sn/sites/rds.refer.sn/IMG/pdf/9b93-11-17ORSEC.pdf Disaster Risk Management in Senegal: Critical analysis of contingency plans https://acasis.locean-ipsl.upmc.fr/lib/exe/fetch.php?media=yanon_revue_critique_des_plans_de_contingences_au_se_ne_gal.pdf
	D1-4 Crisis Management	**Start-up**	No official planning and evaluation of crisis management protocols and	

			procedures are in place. Equally, there is no mandate for risk management planning.	
	D1-5 Cyber Defence Consideration	**Start-up to Formative**	Senegal does not have a specific national cyber defence policy or strategy. Various efforts of the Army and Gendarmerie are conducted on an ad-hoc basis, but there is no strategic coordination between these efforts, nor external engagement outside of the Task Force.	
	D1-6 Digital Redundancy	**Formative**	There are various redundancy efforts within the private sector, including the creation of continuity plans in the event of a crisis. However, the dissemination of such plans, as well as the coordination of efforts between the public and private sectors is currently lacking.	
Dimension 2 Cyber Culture and Society	**D2-1 Cybersecurity Mindset**	**Start-up to Formative**	A cybersecurity mind-set is adopted inconsistently and not engrained across society. Cybersecurity is a concern, but mainly for IT experts within government rather than for general staff or managers. Within some large private sector organisations, such as telecommunication companies or banks, an increasing understanding of cybersecurity threats and risks is developing. However, most private sector entities do not recognise the need for cybersecurity yet. Society at-large is unaware of cyber threats.	
	D2-2 Cybersecurity Awareness	**Formative**	There is no coordinated programme or campaign at a national level in Senegal to cover all groups in society with defined targets and goals. Current awareness raising efforts by academia and civil society are fragmented. Moreover, there is no promotion of safety online at a national level.	
	D2-3 Confidence and trust on the Internet	**Start-up to Formative**	Trust in online services is identified as a concern. Measures to promote trust in online services have not yet been implemented. Users do not have enough knowledge regarding safe online practices and data protection. Online services are often used in "blind" trust or distrust, while an	E-government services provided by ADIE http://servicepublic.gouv.sn/

			informed formation of trust is lacking. E-government services are under development, but there is no coordinated effort to promote trust in e-government services. Uptake of e-commerce and e-banking services in Senegal is still low.	
	D2-4 Privacy Online	**Start-up to Formative**	Comprehensive privacy and data protection legislation has been adopted. However, implementation of the legislation is insufficient and private sector employers do not recognise privacy as an important component of cybersecurity.	Law No. 2008-12 on the Protection of Personal Data (2008) http://www.cdp.sn/images/doc/protection.pdf The Right to Privacy in Senegal: Stakeholder Report (Privacy International and Jonction Senegal, 2013)
Dimension 3 Cybersecurity Education, Training and Skills	**D3-1 National Availability of Cybersecurity Education and Training**	**Formative**	The educational offerings available in information security are limited. National universities offer technical educational programmes, for instance relating to cryptography, with cybersecurity components, but there are no specialised cybersecurity study programmes and no offerings below university level. Some academic and private sector providers offer cybersecurity specific courses or training programmes, but these are largely ad-hoc and fragmented.	Cheikh Anta Diop University http://edmi.ucad.sn/index.php?option=com_content&view=article&id=22&Itemid=27 African Center of Excellence in Mathematics, Computer Science and ICT (CEA-MITIC) at the Université Gaston Berger - Saint-Louis http://www.ceamitic.sn/index.php University of Bambey http://www.uadb.edu.sn/index.php/formation Virtual University of Senegal http://www.uvs.sn/
	D3-2 National development of cybersecurity education	**Formative**	Academia is the main driver of developing education and training offerings. However, a nationally coordinated programme is still lacking.	
	D3-3 Training and educational initiatives within public and private sector	**Formative**	Cybersecurity training programmes for employees are usually limited to IT-related staff. Although IT staff sometimes share knowledge and skills in and ad-hoc manner, training programmes for general staff and knowledge sharing initiatives have not yet been institutionalised.	

	D3-4 Corporate Governance, Knowledge and Standards	**Formative**	Within certain sectors, such as banking, executive-level senior management has an understanding of cybersecurity risks, but overall, the knowledge and awareness of direct cybersecurity threats and their potential impact on the organisations is limited. It is generally common for boards to rely on IT-departments.	
Dimension 4 Legal and Regulatory Frameworks	**D4-1 Cybersecurity Legal Frameworks**	**Formative to Established**	A legislative and regulatory cybersecurity framework was established in 2008. ICT security is regulated in *Law No. 2008-10 on Orientation Law on Information Society*, *Law No. 2008-08 on Electronic Transactions*, and *Law No. 2008-41 on Cryptology*. The protection of privacy has been engrained in the Constitution of Senegal. *Law No. 2008-12 on the Protection of Personal Data* provides a comprehensive data protection framework. Substantive and procedural cybercrime provisions are contained in *Law No. 2008-11 on Cybercrime*. Senegal is in the process of accession to the Budapest Convention and has implemented the ECOWAS Directive on Fighting Cyber Crime. However, the implementation of this legal framework varies and is generally not sufficient. Moreover, since 2008, no amendments have been passed to the laws, which has led to gaps and a discrepancy between the legal provisions and the reality of cybersecurity in Senegal.	Constitution of the Republic of Senegal (2001) http://www.gouv.sn/-Constitution-du-Senegal-.html Law No. 2008-10 on Orientation Law on Information Society (2008) http://www.cdp.sn/images/doc/LOSI.pdf Law No. 2008-08 on Electronic Transactions (2008) http://www.cdp.sn/images/doc/transactions.pdf Law No. 2008-11 on Cybercrime (2008) http://www.cdp.sn/images/doc/cybercrime.pdf Law No. 2008-12 on the Protection of Personal Data (2008) http://www.cdp.sn/images/doc/protection.pdf Law No. 2008-41 on Cryptology (2008) http://www.cdp.sn/images/doc/crytologie.pdf Overview of ICT legislation (ADIE) http://www.adie.sn/fr/r%C3%A9glementation-des-tic The Right to Privacy in Senegal: Stakeholder Report (Privacy International and Jonction Senegal, 2013)

				Senegal: Analysis of selected Internet regulation (Article 19, 2015) https://www.article19.org/data/files/medialibrary/37908/Senegal-legal-analysis-EN.pdf Current ICT Initiatives and projects - Republic of Senegal (IST Africa) https://www.ist-africa.org/home/default.asp?page=doc-by-id&docid=5557
	D4-2 Legal investigation	**Start-up to Formative**	Law enforcement have some capacity to investigate computer related crimes, in accordance with domestic law, however this is minimal. Prosecutors are found to lack adequate training and the necessary capacity to prosecute computer related crimes is not in place. There is no separate court structure or specialized judges for cybercrime cases and electronic evidence. Judges do not have the capacity to preside over a case on cybercrime.	GLACY project http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/COE_Cybercrime_List_2014_v1.pdf Homeland Security Policy (Ministry of Interior and Public Security) http://www.interieur.gouv.sn/securite-interieure/politique-de-securite-interieure/
	D4-3 Responsible Reporting	**Start-up**	No official responsible disclosure framework or policy has been established.	
Dimension 5 Standards, organisations, and technologies	**D5-1 Adherence to standards**	**Start-up to Formative**	Cybersecurity standards have been identified for use and some standards, such as ISO/IEC 27001 are adhered to within some parts of public and private sectors. However, different departments within the government and organisations adhere to different standards according to their needs, customer demands and requirements imposed by international parent organisations, rather than government regulations. The implementation of standards in procurement and software development practices do not yet fully meet international IT guidelines, standards and acceptable practices.	
	D5-2 National Infrastructure Resilience	**Formative**	Internet services infrastructure is increasingly reliable, leading to the growing use of the Internet for varied	

			purposes. National infrastructure resilience is managed primarily by ARTP, but coordination with the private sector is still low.	
	D5-3 Cybersecurity Marketplace	**Start-up**	The cybersecurity marketplace is underdeveloped. Foreign technologies are being deployed instead of producing security products domestically. The need for developing a cybercrime insurance market was not yet identified at a national level.	

Table II: Recommendations

Dimension	Capacity Factor	Current Stage of Maturity	Recommendations to Enhance Stage of Maturity
Dimension 1 Cyber Security Policy and Strategy	**D1-1 National Cybersecurity Strategy**	**Strategic**	• **R1-1:** Embark toward developing a National Cybersecurity Strategy to set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. This strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives. • **R1-2:** Allocate a specific mandate for the implementation of the National Cybersecurity Strategy. • **R1-3:** Design and disseminate a coordinated cyber programme. • **R1-4:** Strengthen and promote inter-departmental cooperation in cybersecurity.
	D1-2 Incident Response	**Established**	• **R1-5:** Categorise and record national-level cyber incidents in a central registry. • **R1-6:** Work towards the development of a national CSIRT with clear processes and defined roles and responsibilities. • **R1-7:** Draft legislation which allocates mandates to the national CSIRT. • **R1-8:** Develop a coordination and information sharing mechanism between the private and the public sector. • **R1-9:** Appoint and publicize a national-level lead to ensure reporting of incidents and promote reporting. • **R1-10:** Define lines and channels of communication for crisis situations within the government.
	D1-3 Critical National Infrastructure	**Established**	• **R1-11:** Develop a national list of Critical National Infrastructure (CNI) assets with identified risk based priorities. • **R1-12:** Establish a mechanism for regular vulnerability disclosure and information sharing between the public and private sector. • **R1-13:** Establish information protection and risk management procedures and processes, supported by adequate technical security solutions, which inform the development of an incident response plan. • **R1-14:** Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CNI

			operators. • **R1-15:** Allocate budget for conducting emergency response scenario exercises.
	D1-4 Crisis Management	**Established**	• **R1-16:** Conduct a needs assessment of measures that require testing with consideration of a simple exercise scenario. • **R1-17:** Allocate a mandate for planning of exercises. • **R1-18:** Include all stakeholders in the planning and evaluation of the exercises. • **R1-19:** Conduct compromised communication scenarios and exercises to test emergency response assets interoperability and function effectively. • **R1-20:** Evaluate the exercises and feed the findings back into the decision-making process
	D1-5 Cyber Defence Consideration	**Established**	• **R1-21:** Commence the development of a Cyber Defence Strategy which takes into consideration identified threats to national security in cyberspace. • **R1-22:** Develop a central command and control centre or structure for cyber defence. • **R1-23:** Enhance coordination in response to malicious attacks on military information systems and critical national infrastructure. • **R1-24:** Conduct consistent review of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.
	D1-6 Digital Redundancy	**Established**	• **R1-25:** Allocate appropriate resources to not just hardware integration, technology stress testing, personnel training and crisis simulation drills, but also on ensuring redundancy efforts are appropriately communicated. • **R1-26:** Hardwire all emergency response assets into a national emergency communication network. • **R1-27:** Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.
Dimension 2 Cyber Culture and Society	**D2-1 Cybersecurity Mind-Set**	**Formative**	• **R2-1:** Enhance efforts at all levels of government to promote understanding of risks and threats, but also to design systems that enable users across society to more easily embed secure practices into their everyday use of the Internet and online services. • **R2-2:** Work on promoting sharing of information on incidents and best practices among organisations to

			promote a proactive cybersecurity mind-set. • **R2-3:** Promote prioritisation of risk and threat understanding for private sector entities by identifying high-risk practices. • **R2-4:** Develop programmes and materials to train the public and improve cybersecurity practices.
	D2-2 Cybersecurity Awareness	**Established**	• **R2-5:** Develop a national awareness raising programme to cover various target groups, focusing on the most vulnerable users. • **R2-6:** Link the development of the programme to the process of the national cybersecurity strategy development. • **R2-7:** Engage multiple stakeholders in the development and delivery of the awareness raising programme.
	D2-3 Confidence and trust on the Internet	**Formative**	• **R2-8:** Expand e-government services with recognition of the need for the application of security measures to promote trust in e-services. • **R2-9:** Promote adherence to cybersecurity protection standards for e-government services. • **R2-10:** Promote the need for security in e-commerce services.
	D2-4 Privacy Online	**Established**	• **R2-11:** Promote understanding and initiate discussions regarding the implementation of privacy standards and policies within government. • **R2-12:** Sensitise private sector leaders and employees on employee privacy rights and obligations.
Dimension 3 Cybersecurity Education, Training and Skills	**D3-1 National Availability of Cybersecurity Education and Training**	**Established**	• **R3-1:** Engrain cybersecurity training and education throughout all levels of education. • **R3-2:** Allocate additional resources to cybersecurity education and training for public universities. • **R3-3:** Identify training needs and develop training courses, seminars and online resources for targeted demographics, such as users and experts. • **R3-4:** Create cybersecurity career opportunities and promote the attractiveness of cybersecurity careers to wider leadership roles.
	D3–2 National development of cybersecurity education	**Established**	• **R3-5:** Develop a nationally coordinated programme on cybersecurity education and skills development. • **R3-6:** Allocate budget for training and research and development in cybersecurity, and start multi-stakeholder discussions on how to promote

			cybersecurity as a 'profession' with clear career pathways. • **R3-7:** Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy. • **R3-8:** Create obligatory cybersecurity modules for students and teachers in order to promote knowledge in cybersecurity and create an interest for careers in cybersecurity.
	D3-3 Training and educational initiatives within public and private sector	**Established**	• **R3-9:** Establish basic requirements for cybersecurity training for the public and private sectors. • **R3-10:** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools. • **R3-11:** Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms.
	D3-4 Corporate Governance, Knowledge and Standards	**Established**	• **R3-12:** Conduct mandatory cybersecurity trainings for board members to enhance the understanding of the overall organisational business risk from cyber threats, in a regular manner. • **R3-13:** Promote cooperation and communication channels between technicians and CEO's to transfer the need for investment in cybersecurity.
Dimension 4 Legal and Regulatory Frameworks	**D4-1 Cybersecurity Legal Frameworks**	**Dynamic**	• **R4-1:** Review and amend existing laws on cybersecurity, data protection and cybercrime to address gaps and overlaps. • **R4-2:** Fully ratify and implement regional and national cybercrime instruments, including through the allocation of sufficient resources according to national priorities. • **R4-3:** Review and improve legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime.
	D4–2Legal investigation	**Strategic**	• **R4-4:** Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody. • **R4-5:** Develop and institutionalise specialised training programmes for police, prosecutors and judges in computer related crime. • **R4-6:** Establish and strengthen formal and informal international cooperation mechanisms within the

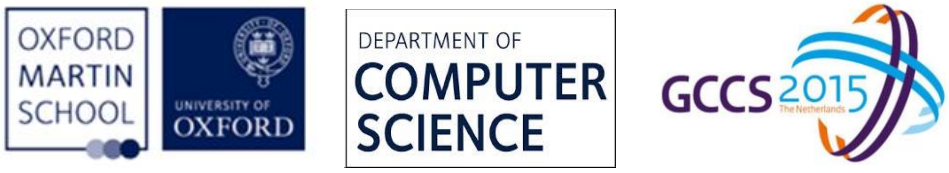
			police and criminal justice system.
	D4-3 Responsible Reporting	**Formative**	• **R4-7:** Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledgement report. • **R4-8:** Encourage sharing of technical details of vulnerabilities among CNI.
Dimension 5 Standards, organisations, and technologies	**D5-1 Adherence to standards**	**Established**	• **R5-1:** Establish a programme to strengthen government's capacity to adapt or adopt international standards in order to acquire a baseline in the context of organisational cybersecurity. • **R5-2:** Promote adoption of international IT standards, in particular during procurement, software and code development. • **R5-3:** Promote the awareness and implementation of standards among SME.
	D5–2National Infrastructure Resilience	**Established**	• **R5-4:** Increase reliability of online government services and promote their full deployment. • **R5-5:** Develop a national programme for infrastructure development. • **R5-6:** Work on enhancing the level of security processes in place (threat assessments and risk management processes). • **R5-7:** Invest in ICT research and cooperation between academia, research and industry to strengthen the software-engineering competencies of domestic ICT companies.
	D5-3 Cybersecurity Marketplace	**Established**	• **R5-8:** Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development. • **R5-9:** Promote sharing of information and best practices among organisations, to continue to explore potential cybercrime insurance coverages.

Lead Editors and Authors

Mr Taylor Roberts
Ms Eva Ignatuschtschenko

Authors (listed alphabetically)

Ms. Lara Pace
Professor Basie Von Solms



Global Cyber Security Capacity Centre
Oxford Martin School, University of Oxford
Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,
United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk
Portal: https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home