CYBERSECURITY CAPACITY REVIEW

The Gambia

April 2019

Global Cyber Security Capacity Centre
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD
THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Mr Óscar Noé Ávila Molina, Mr Bonyaminou Porrogho, Dr Eva Nagyfejeo

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Professor Basie Von Solms, Professor Federico Varese, Dr Jamie Saunders

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*19/12/2018*	*First draft submitted to Technical Board*
2	*13/02/2019*	*Second draft submitted to World Bank*
3	*19/02/2019*	*Second draft submitted to MOICI and PURA*
4	*19/04/2019*	*Third draft submitted to World Bank, MOICI and PURA*

LIST OF ABBREVIATIONS

ACE Submarine Cable	Africa Coast to Europe Submarine Cable
ARIPO	African Regional Intellectual Property Organization
CCNA	Certified Cisco Network Associate
CCNP	Certified Cisco Network Professional
CI	Critical Infrastructure
CID	Criminal Investigation Department
CIRT	Computer Incident Response Team
CMM	Cybersecurity Capacity Maturity Model
CPA	Consumer Protection Act
CSIRT	Computer Security Incident Response Team
ECOWAS	Economic Community of West African States
GCCPC	Gambia Competition and Consumer Protection Commission
GCSA	Gambia Cyber Security Alliance
GCSCC	Global Cyber Security Capacity Centre
GM-CSIRT	Gambia CSIRT
GPF	Gambia Policy Force
ICA	Information Communications Act
ICT	Information and Communication Technologies
IGO	Intergovernmental Organisation
(ISC)2	International Information System Security Certification Consortium
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunications Union
MOICI	Ministry of Information and Communication Infrastructure
NCI	National Critical Infrastructures
NCSA	National Cybersecurity Authority
NCSC	National Cybersecurity Committee
NCSS	National Cybersecurity Strategy
NDMA	National Disaster Management Agency
NDP	National Development Plan 2018-2021

NGO	Non-governmental Organisation
NICI	Communication Infrastructure Policy
NSC	National Security Council
NSP	National Security Policy
PII	Personal Identification Information
PURA	Public Utilities Regulatory Authority
SME	Small and medium-size Enterprise
TDOC	Taiwan Digital Opportunity Centre
WB	World Bank
WIP	World Intellectual Property Organisation
WIPO	World Intellectual Property Organisation
WPO	World Trade Organization

EXECUTIVE SUMMARY

In collaboration with the World Bank (WB), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in The Gambia at the invitation of the Ministry of Information and Communication Infrastructure (MOICI). The objective of this review was to enable The Gambia to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period 31 October–2 November 2018, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies the banking sector as well as international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cyber Culture and Society*
- *Cybersecurity Education, Training and Skills*
- *Legal and Regulatory Frameworks*
- *Standards, Organisations, and Technologies*

Each dimension comprises *factors* which describe what it means to possess cybersecurity capacity. Factors each present a number of *aspects* which group together related *indicators*, which in turn describe steps and actions that, once observed, define the stage of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in The Gambia and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

[1] Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (assessed 25 February 2018)

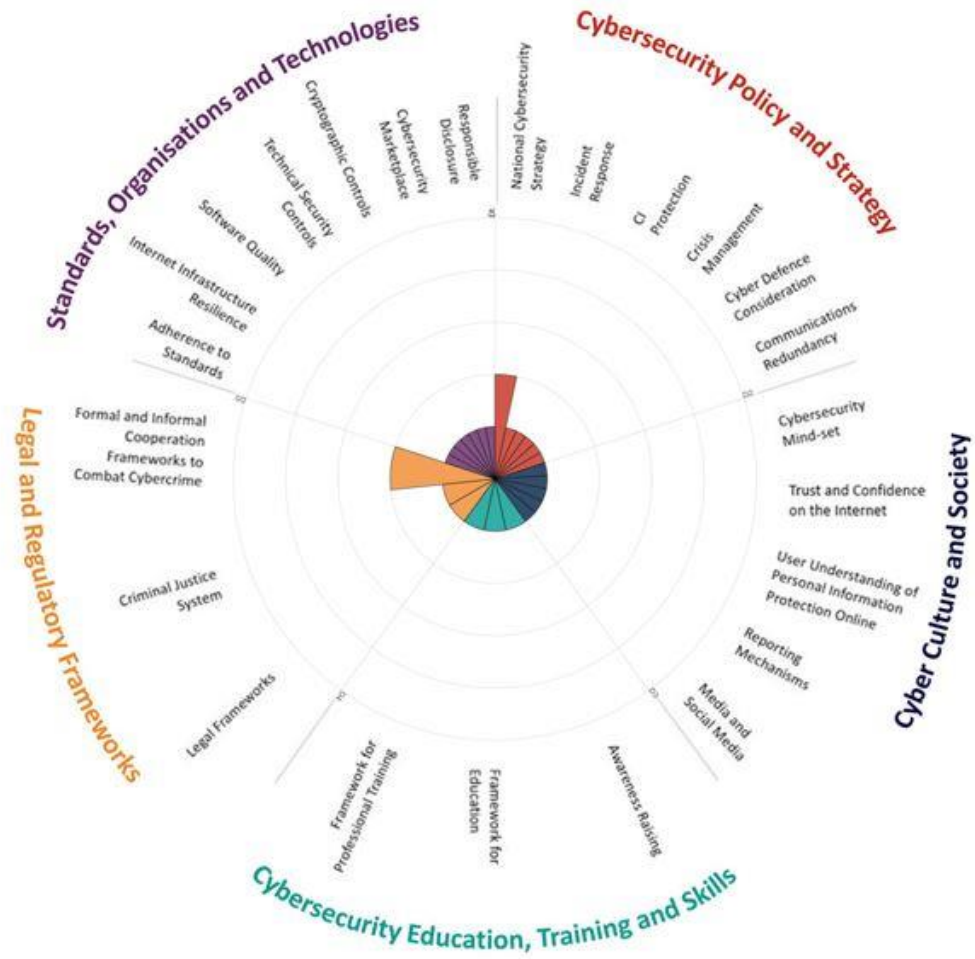

Figure 1: Overall representation of the cybersecurity capacity in The Gambia

Cybersecurity Policy and Strategy

Through CMM review sessions, the cybersecurity policy and strategy dimension of cybersecurity capacity for The Gambia was identified to range from start-up to formative stages of maturity.

Currently, The Gambia does not have a national cybersecurity strategy in place. However, a cybersecurity strategy was drafted back in 2016 but it has not been adopted yet. MOICI and PURA are leading the cyber initiatives as cyber task force. These two actors have been working closely with the ITU, World Bank and other partners to create the national computer security incident response team. GM-CSIRT would be set up the first quarter of 2019 and is expected to reach an operational level by the end of 2019.

No regulation that requires cyber incidents to be reported is in place and The Gambia lacks a mandated authority or protocol to handle and manage such reporting mechanisms and process.

The draft of the national cybersecurity strategy contains a central list of critical infrastructure (CI) assets which has not been made official by the Gambian authorities. Communication

between the government and CI operators is ad-hoc and therefore coordination is very limited. In cases where a coordinated response would be required, neither a cybersecurity operational strategy or contingency plan, nor an official mandate is in place to manage and mitigate the adverse consequences of cyber incidents.

Similarly, risk management exercises or cyber drills are not conducted at a national level. In the case of crisis management, national planning and evaluation of crisis management protocols and procedures are in place, but as yet these plans and evaluations do not incorporate cyber components. Therefore, cybersecurity has not been integrated in the crisis management system of The Gambia.

No evidence of the existence of a national defence policy or strategy. However, cyber threats are starting to be recognised in the national security landscape. Apparently, there is no strategic coordination or command and control structure for cyber Defence and operational capacity has not yet been developed. Based on the current government posture, it is likely that cyber defence actions and initiatives would become a priority for the country and would eventually be addressed in the future national defence policies or strategies.

Communications redundancy as a broad concept has been considered in The Gambia, resulting in sectoral actions to backup data and established redundant networks in cases of communication breakdown. Coordinated and systematic actions have been taken at the organisational and business level, but none at the national level.

Cyber Culture and Society

The Consultations have indicated that the national capacity, of the Gambia, in the cybersecurity culture and society dimension was still at a Start-up level.

At a governmental level, cybersecurity was identified as a concern, but it was noted that the majority of employees and high-level officials have a low level of cybersecurity threat awareness.

Some large organisations in the private sector, such as telecommunications operators and banks, possess some understanding of cybersecurity threats and risks and are taking initiatives in 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 with defined targets and goals.

E-government services are not offered in the Gambia and the use of online banking services and e-commerce services is still low despite some popularity of mobile payment solutions. The knowledge of users regarding safe online practices is limited, which have 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 is still to be adopted and the recognition of privacy as an important component of cybersecurity in general is still low.

Cybersecurity Education, Training and Skills

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. Due to the lack of a national awareness programme, cybersecurity awareness amongst the general public is low. The need for awareness raising programmes has been recognized by the government in the draft national cybersecurity strategy (NCSS), however the final NCSS draft was not officially adopted yet.

The Gambia Cyber Security Alliance (GCSA) – a civil society organization with a view to promote, advocate and create awareness on cyber security - conducts cybersecurity awareness campaign and seminars for officials and the general public. [2] The Alliance is also active at the school level, conducts school and community outreach at the grassroots level in order to talk to users about safety online.

Focus-group discussions suggest that awareness of cybersecurity issues is very limited among executive managers both in public and private sectors, which could be one of the reasons why cybersecurity awareness-raising has not yet been perceived as a priority.

The need for enhancing cybersecurity education in schools and universities has been identified by leading government and academic stakeholders. One of the strategic priorities of the draft NCSC is to ensure the next generation of cybersecurity professionals (Section 5.1.1) though the development of school curriculums concerning cybersecurity.

There is currently no formal cybersecurity education/national curriculum for cybersecurity in The Gambia. Participants confirmed that there is no formal cybersecurity education at the primary or secondary school level.

No cybersecurity framework for certification and accreditation of public-sector professionals exists. Civil society organisations such as GCSA provides ad-hoc cybersecurity professional trainings to police force and the private sector (i.e. banks) to build a culture of cybersecurity.

Legal and Regulatory Frameworks

Legal and regulatory capacities were identified to range between start-up and formative stages of maturity.

The Information Communication Act (2009) is basically a general legal and regulatory framework which governs multiple cyber-related manners, such as privacy protection and personal data processing, computer misuse and cybercrime, children's protection, e-signature, e-transactions, e-government services, among others. However, the country requires a more comprehensive framework to address and tackle issues related to cybercrime -substantive and procedural provisions-, ICT security -critical infrastructure (NCII) - and cybersecurity governance, and not just cybercrime. While such law covers some aspects of cybersecurity, legislative gaps and inconsistent application of law have led to a lack of online protection for consumers, children and even citizens' personal information. Discussions have begun regarding the development of new legislation on cybercrime, but some aspects, such as intellectual property online, are not yet a topic of concern.

[2] Gambia Cyber Security Alliance. Available at http://gamcybersecurityalliance.com/ (Accessed 12/12/2018)

Regarding operational capacities, law enforcement has limited capacities to investigate cyber-related crimes. Specialised and regular training is not widely available for law enforcement officers which limits investigative capabilities.

Prosecutors and judges are not trained adequately. A limited number of prosecutors and judges have basic capacities to prosecute and preside over cyber-related crimes; complex cybercrime cases may be an issue to handle. Lack of a cybercrime procedural law has been one of the major issues to investigate, prosecute and process cases of this nature. Domestic and international cooperation to combat cybercrime is largely informal in nature, in particular through INTERPOL and other regional channels. Formal mechanisms that complement these informal relationships are beginning to be discussed.

Standards, Organisations, and Technologies

The national capacity of the Gambia in Standards, Organisations and Technologies Dimension was identified as start-up.

No coordinated effort to adopt and implement cybersecurity standards was initiated. Some procurement and software development standards might be applied but, overall, the strategic focus is primarily on basic functionalities and price.

Internet services are not yet reliable nor affordable. No evidence of coordination and cooperation, among institutions that are involved in the provision of Internet services, to provide reliable and affordable services was identified.

Software quality is not monitored and there is no catalogue of secure software platforms and applications for the public nor the private sector.

ISPs do not offer anti-malware software as part of their services and users only have a limited understanding of the available technical security controls.

Similarly, cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and in transit have been identified as a concern but are not yet systematically deployed within the government nor the private sector.

While international providers offer a range of cybersecurity products for domestic use, there are no domestic commercial cybersecurity products or cybercrime insurance offerings in the Gambia.

Additional Reflections

Even though the level of stakeholder engagement in the review was more limited than we might have hoped, which limits the completeness of evidence in some areas, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 29th country review that we have supported directly.

INTRODUCTION

At the invitation of Ministry of Information and Communication Infrastructure (MOICI) and in collaboration with the World Bank (WB) the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity of The Gambia. The objective of this review was to enable The Gambia to determine areas of capacity in which the government might strategically invest in, in order to improve their national cybersecurity posture.

Over the period 31 October – 2 November 2018, stakeholders from the following sectors participated in a three-day consultation process:

- Public sector entities
  - Gambia Public Utilities Regulatory Authority (PURA)
  - Ministry of Information and Communication Infrastructure (MOICI)
  - Gambia Competition & Consumer Protection Commission (GCCPC)
  - Ministry of Defense (MoD)
  - Office of The President
  - Gambia Revenue Authority (GRA)
  - Accountant General's Department
  - Ministry of Finance & Economic Affairs
  - Ministry of Transport, Works and Infrastructure (MOTWI)
  - Ministry of Health & Social Welfare (MOHSW)
  - Ministry of Petroleum and Energy (MOPE)
  - Gambia Standards Bureau (TGSB)

- Criminal justice sector
  - Gambia Police Force
  - Gambian Judiciary
  - National Assembly
  - Attorney General's Chambers
  - Ministry of Justice

- Finance sector
  - GT Bank Gambia
  - Financial Intelligence Unit (FIU)
  - Central Bank of the Gambia (CBG)
  - Trust Bank Gambia
  - Reliance Financial Services (RFS)
  - Ecobank
  - Zenith Bank

- Private sector
  - Nifty ICT Solutions
  - Xoom Wireless Gambia
  - Gambia Semlex

- Critical infrastructure owners
  - Gambia Telecommunications Company Limited (GAMTEL)
  - Gambia Submarine Cable (GSC)
  - Unique Solutions
  - Africell National Roads Authority (NRA)
  - Comium Gambia
  - QCell
  - Gambia Telecommunications Cellular Company (GAMCEL)
  - Edward Francis Small Teaching Hospital (EFSTH)
  - Gambia Transport Service Company (GTSC)
  - National Water and Electricity Company (NAWEC)
  - Gambia Civil Aviation Authority (GCCA)
  - Gambia Ports Authority (GPA)

- National Security Agencies
  - State Intelligence Services (SIS)
  - Office of National Security

- Academia, Civil Society
  - University of the Gambia ICT Association (UTGICTA)
  - Association of Non-Governmental Organizations in the Gambia (TANGO)
  - Islamic Online University (IOU)
  - Gambia Technical Training Institute (GTTI)
  - Gambia Ministry of Basic and Secondary Education (MOBSE)
  - Management Development Institute (MDI)
  - Gambia Cyber Security Alliance (GCSA)
  - Internet Society Gambia (ISOC)
  - American International University West Africa (AIUWA)

- International community
  - World Health Organization (WHO)
  - International Organization for Migration (IOM)

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model (CMM)[3] which is composed of five distinct *dimensions* of cybersecurity capacity.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions with the five dimensions together with the factors of which they are comprised:

DIMENSIONS	FACTORS
Dimension 1 Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 Cyber Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 Cybersecurity Education, Training and Skills	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 Legal and Regulatory Frameworks	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 Standards, Organisations, and Technologies	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

[3] See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors each present a number of aspects which gather together related indicators, which in turn describe steps and actions that once observed define which stage of maturity this specific element of aspect is. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **Start-up:** at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.
- **Formative:** some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new However, evidence of this aspect can be clearly demonstrated.
- **Established:** the indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.
- **Strategic:** at this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state's or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication 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. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

The assignment of maturity stages is based upon the evidence collected, including the general or consensus view of accounts presented by stakeholders, desktop research conducted, and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of The Gambia and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of The Gambia and

concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

METHODOLOGY - MEASURING MATURITY

During the country review specific dimensions are discussed with the relevant group of stakeholders. Each stakeholder cluster is expected to respond to one or two dimensions of the CMM, depending on their expertise. For example Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 and Dimension 3 of the CMM.

In order to determine the level of maturity, each aspect has a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions stakeholders should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[4] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[5] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[6]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to

[4] Relevant publications:
Williams, M. (2003).Making sense of social research. London: Sage Publications Ltd. doi: 10.4135/9781849209434
Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. SAGE Focus Editions: Successful focus groups: Advancing the state of the art (pp. 35-50). Thousand Oaks, CA: SAGE Publications Ltd. doi: 10.4135/9781483349008
Krueger, R.A. and Casey, M.A. (2009). Focus groups: A practical guide for applied research. London: Sage Publications LTD.

[5] Relevant publications: J. Kitzinger. 'The methodology of focus groups: the importance of interaction between research participants.' Sociology of Health & Illness, 16(1):103–121, 1994.
J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299– 302, 1995.
E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, pages 1–13, 1982.

[6] J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299– 302, 1995.

the data generated by focus groups.[7] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[8]

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[9] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[10] Dey explains that this process categorises data as "belonging together".[11]

The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.[4]

In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a third, blended approach in the analysis of our data, which is a mixture of deductive and inductive approaches.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and use the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

---

[7] K. Krippendorff. Content analysis: An introduction to its methodology. Sage Publications, Inc, 2004. H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.
K.A. Neuendorf. The content analysis guidebook. Sage Publications, Inc, 2002.

[8] E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, Volume and Number? pages 1–13, 1982.

[9] S. Elo and H. Kyng¨as. 'The qualitative content analysis process.' Journal of Advanced Nursing, 62(1):107–115, 2008.
H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.

[10] P.D. Barbara Downe-Wamboldt RN. 'Content analysis: method, applications, and issues.' Health Care for Women International, 13(3):313–321, 1992.

[11] I. Dey. Qualitative data analysis: A user-friendly guide for social scientists. London: Routledge, 1993.

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders.

Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of The Gambia and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN THE GAMBIA

In 2017, the government of The Gambia recognised the importance of moving from an industrially weak and subsistence agriculture-based economy towards an information and knowledge economy. Under such premise, the government of The Gambia has developed and implemented comprehensive ICT-development policies, strategies and plans to foster and facilitate its economic and social growth.[12]

In 2002, The Gambia launched the ICT for Development (ICT4D) process, phase 1 of the National Information and Communication Infrastructure Policy (NICI-1) in 2004 and the ICT4D action plan in 2010 and phase 2 known as NICI-2 in 2016 (2017-2025).[13]

As a result of the implementation of those policies and strategies, new thematic areas emerged on the ICT4D scene, including Internet broadband and cybersecurity, some lessons learned and specific recommendations on actions to be taken in the next phase of the NICI process, NICI-2. As part of the ICT4D's continuity and mission, The Gambia committed to pursuing the following relevant actions: rapid modernizing and deployment of the requisite national ICT backbone infrastructure, addressing the Nation's cybersecurity capability and affordable broadband access (strategic G) and developing the Nation's cybersecurity capabilities and strength in the information age (strategic I). To facilitate the transformation process of The Gambia into a predominantly information-rich and knowledge-based society and economy, the NICI-2 (2017-2025) established 8 priority policy focus areas, including "promoting advanced broadband ICT infrastructure development and cybersecurity capability".

Internet

The percentage of individuals using the Internet in The Gambia has slowly grown over the past two decades with 18.5% adoption in 2018, compared to 0.92% in 2000.[14] PURA estimates that Internet penetration already reached 19%.[15] Such increase of internet adoption has led to The Gambia being ranked 144th on the International Telecommunications Union (ITU) Global ICT Development Index ranking, which indicated that in 2017 there was 0.18 percent fixed (wired)-broadband subscriptions per 100 inhabitants, compared to 21.26 percent active

[12] National Information and Communication Infrastructure Policy. Available at https://moici.gov.gm/sites/default/files/NICI-2%20Policy%20Statement%20%20-%20FINAL%20REPORT_0.pdf (Accessed 12/10/2018)
[13] Ibid
[14] ICT Statistics Database. Available at https://www.google.com/publicdata/explore?ds=emi9ik86jcuic_#!ctype=l&strail=false&bcs=d&nselm=h&met_y=i99H&scale_y=lin&ind_y=false&rdim=country&idim=country:MK:GM&ifdim=country&tstart=1108252800000&tend=1423785600000&hl=en_US&dl=en_US&ind=false and Freedom on the Net 2018, The Gambia. Available at https://www.refworld.org/docid/5be16b184.html (Accessed 12/10/2018)
[15] National Information and Communication Infrastructure Policy. Available at https://moici.gov.gm/nici-policy (Accessed 12/10/2018)

mobile-broadband subscriptions per 100 inhabitants.[16] According to the World Economic Forum's 2016 Global Information Technology report,[17] The Gambia ranks 123th in the world on Affordability (including the cost of accessing ICT, either via mobile telephony or fixed broadband Internet, as well as the level of competition in the Internet and telephony sectors that determine this cost).

The Gambia is still behind in Internet broadband penetration, especially in mobile Internet deployment which ranks as one of the slower rates in the region; in accessibility, network coverage is restricted to areas where corporate customers are available; in affordability, broadband services are expensive compared to the average earning of the Gambians; in usage of ICT by both public and private sectors, there are almost no applications to help stimulate the demand; and in literacy, more than half of the population are illiterate.[18]

To increase the Internet broadband penetration, The Gambia has been deploying some infrastructure, such as the Fibre Optic Cable, ACE Submarine Cable and the Serrekunda Internet Exchange point, and also working on key policies to give direction to the ICT sector as a whole, including the National Information and Communication Infrastructure Policy (NICI-1 and NICI-2) which guides ICT program/project implementation and aims at enhancing broadband penetration in the country. Additionally, MOICI identified the following components as possible intervention areas: (i) funding for formulating and development of a comprehensive Internet broadband plan, (ii) technical cooperation to enhance the capacity of Gambians in ICTs; (iii) funding for investment to encourage local content development; (iv) funding for the development of an effective real-time monitoring and evaluation framework for broadband penetration; and (v) support the newly developed E-Gambia strategy.[19]

Cybersecurity

The Gambia's cybersecurity capabilities are currently in a start-up stage, some initiatives are more advanced than others, but in essence, none reaches an adequate level of maturity; therefore, the Gambian authorities have a lot of work to do on this domain. In the last decade, The Gambia has at least identified the need of taking some actions to enhance its cyber capabilities and to incorporate cybersecurity in the national agenda.

That's how the NICI-2 incorporated "developing national cybersecurity capability" as one of the pillars; and therefore, The Gambia committed to pursuing certain actions, including but not limited to:

- To develop the Nation's capabilities to rapidly and effectively respond to cyber threats, and reduce the Nation's cybersecurity vulnerabilities, and minimize damages from cyber-attacks and incidents.

[16] ICT Development Index 2017. Available at http://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&GMB (Accessed 12/10/2018)
[17] Global Information Technology Report 2016. Available at http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf (Accessed 12/10/2018)
[18] Increasing Broadband Internet Penetration in the OIC Member Countries. Available at http://www.comcec.org/en/wp-content/uploads/2017/05/9-TRA-PRO.pdf (Accessed 12/10/2018)
[19] Ibid.

- To strengthen the Nation's regulatory and institutional framework to support cybersecurity initiatives and activities.
- To promote, develop, foster and maintain a national culture of security and promote national awareness campaign and capacity building to support cybersecurity mitigating efforts and initiatives.
- To protect and secure the Nation's Critical National Information Infrastructure (CNII)
- To periodically assess, identify and address the Nation's cybersecurity risks, threats, needs and requirements.
- To promote the establishment of cybersecurity institutional governance structures and capabilities.
- To promote the adoption of cybersecurity standards and good practices within government and private sector institutions.

In addition to the above, the newly Gambia National Development Plan (2018-2021) also sets out a series of strategic priorities, including "making The Gambia a digital nation, and creating a modern information society". As part of such national plan, the Gambian government committed to "strengthening cyber-security" by implementing the National Cyber Security Strategy and Action Plan to mitigate cyber threats. The government is also committed to striving to build local capacity including Cyber Defence Systems and personnel to protect national security. This is also aligned with the establishment of the Computer Incidence Response Team (CIRT). The CIRT will be equipped with the necessary resources to avert and combat, not only cyber threats emanating locally but internationally as well.[20]

[20] The Gambia National Development Plan (2018-2021). Available at http://www.thegambiatimes.com/wp-content/uploads/2018/02/1.-The-Gambia-National-Development-Plan-2018-2021-Full-Version.pdf (Accessed 12/10/2018)

REVIEW REPORT

OVERVIEW

In this section, we provide an overall representation of the cybersecurity capacity in The Gambia. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' at the perimeter.

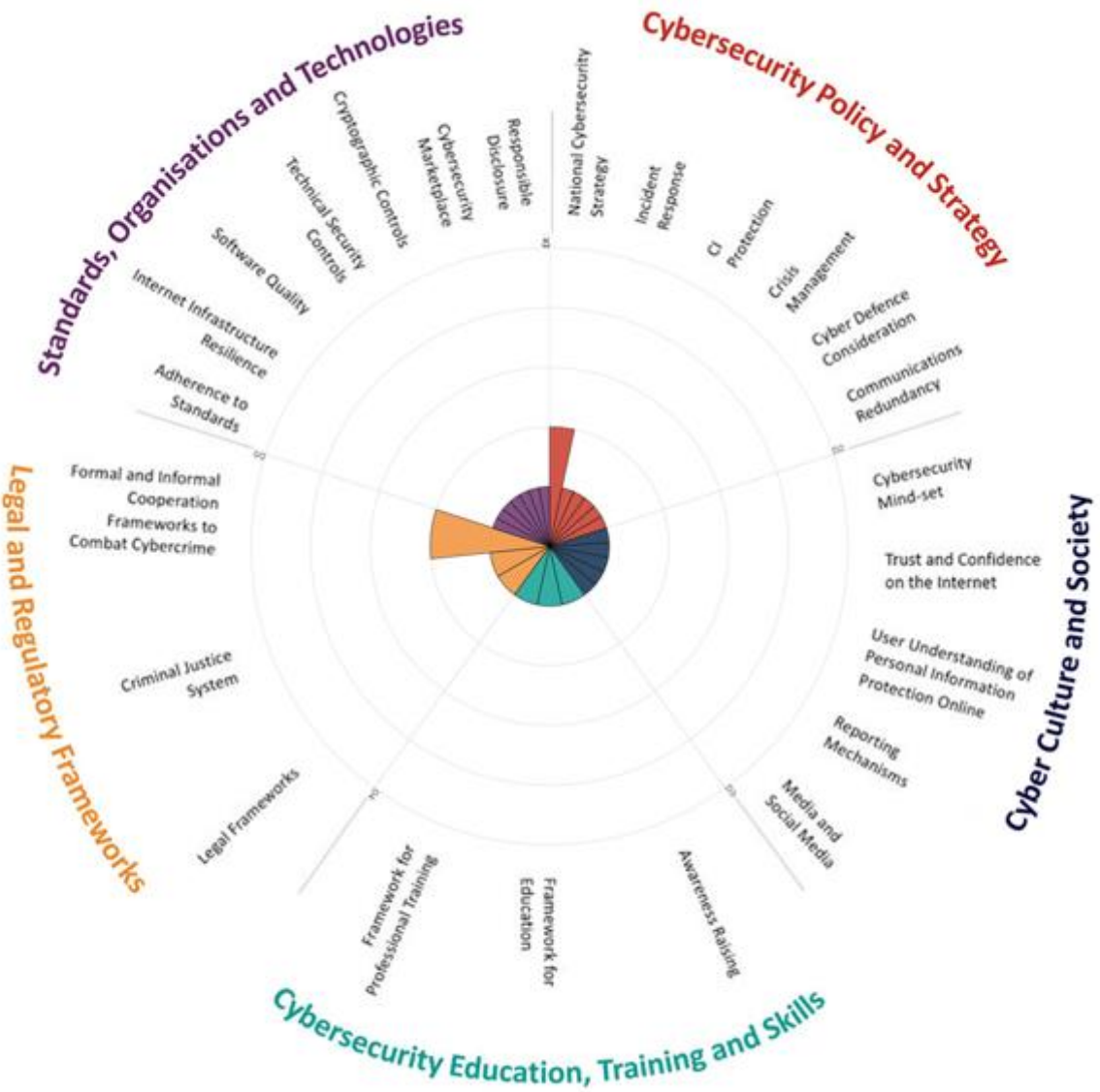

Figure 2: Overall representation of the cybersecurity capacity in The Gambia

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

The factors in Dimension 1 gauge The Gambia's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The Cybersecurity policy and strategy dimension also includes considerations for early warning, deterrence, defence and recovery. This dimension considers effective policy in advancing national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace increasingly vital for government, international business and society in general.

D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government, because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

Stage: Formative

Currently, there is no official national cybersecurity strategy nor a formal national cybersecurity program in place. However, in 2015 the former government of Gambia announced the development of a national cybersecurity strategy (NCSS) whose final draft was finalised[21] and validated by stakeholders in 2016. In 2017, MOICI was in a transition period which caused that such NCSS draft was not officially adopted. Since then, the NCSS draft has not been revised, updated nor submitted for Cabinet´s approval.

[21] COE - Octopus Cybercrime Community. The Gambia Profile. https://www.coe.int/en/web/octopus/country-wiki1/-/asset_publisher/hFPA5fbKjyCJ/content/gambia?inheritRedirect=false (Accessed 12/10/2018)

According to some government's representatives, multiple stakeholders from the public and private sectors (e.g. telecommunications sector, financial sector, government agencies, among others) participated in the discussion during the consultation sessions and their inputs and recommendations were considered and stated in such NCSS draft. However, none of the stakeholders, especially from the private sector, which participated in the CMM review sessions was aware of the existence of the NCSS draft and none of them remembered that their organisations would have participated in those consultation sessions. At the time of the CMM review, such situation raised some concerns with respect to which stakeholders actually participated in the NCSS consultation process and whether their inputs and recommendations were in reality considered in the NCSS draft.

The NCSS draft, which is not currently available online, is based on six key elements: i-) people and entities mobilised to secure their own ICT systems; ii-) people and entities in capacity to provide cybersecurity technology and services; iii-) a national cybersecurity centre acting as a centre of competence and an operational centre; iv-) police forces and justice in capacity to fight against cybercrime; v-) awareness, training and education for all stakeholders; and vi-) a national cybersecurity governance.[22] Furthermore, the NCSS draft is focused on five priority goals: the first two priorities are to build capacity of people, both users and professionals, and provide The Gambia with an institutional framework specific cybersecurity. The third priority is to ensure that ICT systems are protected and made resilient. The fourth priority is to provide The Gambia with a comprehensive legal and regulatory framework. And the fifth priority is to ensure national and international cooperation.

Despite the NCSS draft has not been adopted yet, at least two initiatives related to those key components, the establishment of the GM-CSIRT and the development of a comprehensive cybercrime legislation, have shown a significant advance in the last few years. According to government's representatives, both the cybercrime legislation and the GM-CSIRT will be in place next year; further information would be provided below.

As to the institutional governance, according to the NCSS draft, MOICI, through its Permanent Secretary, will act as the National Cybersecurity Authority (NCSA) which would be in charge of overseeing, implementing and reviewing the NCSS, once adopted. The NCSS draft also contemplates an additional body, the National Cybersecurity Committee (NCSC), which would act as NCSA's advisor and would be in charge of all aspects of the NCSS, from elaboration up to implementation and review. NCSC would be comprised of five subcommittees which would address one specific area each (e.g. public sector, critical infrastructure, law enforcement, national security and civil society) so that most of the relevant stakeholders are expected to be part of the NCSC's decision-making process. NCSC nor any of those subcommittees have been formally established yet. Cabinet's approval would be required to officially establish the NCSC. So far, MOICI has been leading and coordinating the implementation of some initiatives stated in the NCSS draft, and has also delegated some responsibilities to PURA, especially with

[22] CMM review team and World Bank consultants had access to the electronic version of the national cybersecurity strategy labelled as draft 1.6 (13/06/2016).

respect to the establishment of the GM-CSIRT. As stated, various components of the NCSS draft are being implemented, even without NCSS being approved and NCSC being established.

Although the NCSS draft, as a whole, adapted a holistic approach, it is important to highlight that during the last CMM review session, it was highly questioned whether the NCSS draft still addresses The Gambia's demands and priorities in the cybersecurity domain due to it has been there for more than two years without being approved. Government's representatives affirmed that some initiatives are being implemented, for instance the establishment of the GM-CSIRT, but the NCSS draft might not reflect the current demands and situation of the country.

Moreover, the NCSS draft does not make any reference to a budget line for the implementation of the NCSS's strategic goals. MOICI and PURA have not come up with a consolidated budget to allocate resources for NCSS implementation. Currently, MOICI, PURA, and the other ministries and agencies allocate its budget separately and depend on previous experience and future plans to allocate budget for cybersecurity.

Although this aspect is in an incipient stage, it is also important to highlight that government's agencies, such as MOICI and PURA, have taken important actions to implement some relevant initiatives in the cybersecurity domain, and have also sought advice and collaboration from regional and international partners (e.g. ECOWAS, GCSCC, World Bank, Commonwealth, Council of Europe, ITU, among others) to enhance the government, business and citizens' cybersecurity capacities.

D 1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise 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 at the national level. Those incident response organisations are mostly organized and structured as Computer Security Incident Response Teams (CSIRT), Computer Emergency Response Teams (CERT) or Computer Incident Response Teams (CIRT).

Due to the lack of a central organisation, there is no organisation in charge of not only holding a centralised registry of national level incidents but also serving as a national focal point for coordinating incident response to cyberattacks in the country. For instance, if a mobile user wants to report an incident, such user would usually contact either the operators (Africell, Gamcel, etc.), the regulator (PURA) or the consumer protection agency (Gambia Competition

and Consumer Protection Commission), rather than a body specifically tasked with incident response functions.

At the government level, cyber incidents (e.g. Government websites defacement, email phishing, etc.) are managed internally without reporting any supervising agency or following any coordinated and formal procedures, protocols or standards. It is likely that certain public and private organisations, including critical infrastructure operators, are being attacked but they are not aware of this situation since they do not have the tools, mechanisms and expertise to prevent, detect, manage and respond to cyber incidents.

One of the critical enablers set out by The Gambia National Development Plan 2018-2021 (NDP) is indeed ICT and data for development: Making The Gambia a Digital Nation and creating a modern information society[23] which includes the component of strengthening cybersecurity. Such component embraces, among others, the establishment of the Computer Incidence Response Team which "will be equipped with the necessary resources to avert and combat, not only cyber threats emanating locally, but internationally as well."[24] Although NDP was approved this year, The Gambia has been working on establishing a national CSIRT for more than 7 years.

In 2011, ITU[25] conducted a CSIRT assessment in order to determine the readiness of The Gambia to implement a national CSIRT.[26] In 2014, MOICI signed a Memorandum of Understanding with ITU in order to initiate the process of establishing a national CIRT in the Gambia. This project was funded by ITU and World Bank through the WARCIP project.[27]

After ITU technical assistance which aimed to build and deploy technical and other capabilities, The Gambian national CSIRT project (GM-CSIRT) is currently at an advanced stage. Government's representatives estimate that such national CIRT would start operations, with the assistance of ITU, early in 2019, and it would reach an operational level by the end of 2019.

According to the NCSS draft, GM-CSIRT would act as the governmental and national operational centre, and would be under the supervision of the NCSA. It is important to highlight that GM-CSIRT would eventually have the official mandate, according to the NCSS draft, to act and react to cybersecurity incidents or threats targeting The Gambia's government ICT, and all government entities of The Gambia and national critical infrastructure operators are required to report serious incidents to GM-CSIRT.

Moreover, NCSS draft also states that GM-CSIRT would have the following functions: i-) provide early warnings, alerts, announcement and dissemination of information to relevant stakeholders about ICT vulnerabilities, risks and incidents; ii-) inform the relevant authorities in the event of an incident on an ICT-based systems; iii-) provide expertise to cybercrime prosecutors and investigators and preserve digital evidence; iv-) provide cybersecurity guidance to the national critical infrastructure operators; v-) interact across industry, academia and public sector to raise cybersecurity awareness and education and to train

[23] See *supra* note 20.
[24] Ibid.
[25] ITU – Resolution 58. Encouraging the Creation of National Computer Incident Response Teams. Available at https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2012-PDF-E.pdf (Accessed 12/10/2018)
[26] ITU – National CIRT. Available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Gambia.pdf (Accessed 12/10/2018)
[27] PURA Annual Report and Financial Statement 2014. Available at http://www.pura.gm/wp-content/uploads/2018/01/Annual-Report_2014.pdf (Accessed 12/10/2018)

stakeholders in the field of cybersecurity; and vi-) establish connections, exchange of information, participate in cyber drills and also cooperate with international CSIRT organisations and neighboring national CSIRTs.

Once the GM-CSIRT is fully operational, supposedly by the end of 2019, The Gambia would make an important step not only to detect and respond to cyber incidents at the national level but also to effectively protect critical infrastructures and fight against cybercrime. As to the latter, GM-CSIRT would be an important to tool to help enforcing the cybercrime-related provisions of the Information and Communications Act 2009,[28] and also to set out coordination and collaboration mechanisms at the regional and international level (e.g. other national CSIRTs, law enforcement agencies, etc.) in order to facilitate the investigation and prosecution of domestic and cross-border cybercrime incidents.

In 2017, the current President of the Gambia, Mr. Adama Barrow, launched the National Security Council (NSC).[29] Although NSC is a new agency and still in an infancy stage, the National Security Adviser announced in September of 2018 that the first ever National Security Policy (NSP) is being developed. NSP would help the Gambian government to have a more structured and defined approach, and to develop a response system and measures to provide security to the nation.

NSP will focus on five thematic areas, including threats and challenges at national level.[30] As a result of such component, internal and external challenges have been assessed and cyber risks were identified as one source of threats to the national security. Since consultation is still in process, it is highly recommended that government agencies, such as MOICI and PURA, get involved in the consultation process in order to raise all cyber-related issues, especially those associated with the disruption of the critical infrastructures and services, and also to align the NSP with the NCSS draft and GM-CSIRT's functions to avoid duplication of functions and set out collaboration mechanisms at the national level.

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

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

Stage: Start-up

The concept of cybersecurity in critical infrastructure (CI) is in its infancy. Currently, The Gambia has identified at least 9 National Critical Infrastructure (NCI) sectors, but no officially

[28] Information and Communications Act 2009. Available at http://www.pura.gm/wp-content/uploads/2018/01/IC-Info-Comms-Act-2009.pdf (Accessed 12/10/2018)
[29] The Point Digital Newspaper. Available at http://thepoint.gm/africa/gambia/article/president-barrow-launches-the-national-security-council (Accessed 12/10/2018)
[30] The Point Digital Newspaper. Available at http://thepoint.gm/africa/gambia/article/1st-ever-national-security-policy-in-the-pipeline (Accessed 12/10/2018)

recognised yet. According to government's representatives, MOICI led an initiative between 2015 and 2016 to identify The Gambia's critical infrastructures with the intention of ascertaining a list of the current critical infrastructures, including ICT systems, to be incorporated into the NCSS draft.

The NCSS draft defines what is considered a critical infrastructure,[31] including an ICT system, and also provides a list of 9 critical sectors which can be found in both public and private owned and managed infrastructures: i-) banking and finance; ii-) information and communications; iii-) power and energy; iv-) health services; v-) water and food services; vi-) national defence and security; vii-) transport; viii-) government; and ix-) emergency services. Government's representatives manifested that such list of critical infrastructure sectors is just a proposal, no official decision has been made yet. Additionally, the NCSS draft states that a regulatory and methodological framework would be officially established to identify both the NCI and the National Critical Information Infrastructure (NCII)[32], and that specific processes and controls (e.g. obligation to report cyber incidents to GM-CSIRT, setting up minimum compliance standards and requirements, carrying out independent cybersecurity audits, among other) defined by NCSA would be implemented by operators of those critical sectors.

Since GM-CSIRT is not currently operating, the mechanisms for threat and vulnerability disclosure do not exist, and also there are no formal communication channels or collaboration mechanisms have been established; therefore, the interaction on cybersecurity issues between CI owners and operators, and the Government and among CI owners and operators do not exist or is carried out informally. According to participants, information-sharing is very ad-hoc and informal, and international standards and protocols are not followed to share and disclose sensitive or confidential information.

D 1.4 CRISIS MANAGEMENT

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Start-up

Very little was said in the CMM review about cybersecurity crisis management efforts. As stated above, NSC just started to identify cyber incidents as a national security issue and NCSA and GM-CSIRT are not in place yet to lead and coordinate crisis management actions.

[31] *"Infrastructure and assets the loss or compromise of which could result in a major detrimental impact on national security, national defence, the functioning of the state or major essential economic, safety, public health or other social services".* NCSS draft, glossary.
[32] *". . . assets, data, flows or networks which are vital for achieving the services provided by the National Critical Infrastructure".* Article 1.2. of the Proposal for Legal Implementation.

The Gambia National Disaster Management Agency[33] (NDMA), a focal point which serves as the secretariat to the National Disaster Management Council, has been established to operate as the central planning, coordinating and monitoring agency for all disaster management, including natural and man-made disasters, risk reduction activities, and post-disaster recovery at the national level.[34] The Gambia has developed a National Policy on Disaster Management, a Strategic Framework, a National Disaster Risk Management Plan and a Multi-Hazard Contingency Plan;[35] however, NDMA is not equipped with any official mandate to manage and coordinate cyber-related incidents nor such policies and strategies integrate the cybersecurity component in the national crisis management system Therefore, The Gambia does not have an official and coordinated emergency response plan or business-continuity plan focused on cyber issues for national crisis or disasters, including incidents affecting critical infrastructures. Evidence shows that coordinated cyber exercises and simulations are not conducted at the national level in the country.

According to some stakeholders, crisis management related to cyber-related events are sometimes conducted at the organisational level, but these measures are ad-hoc and vary depending on the organisation and its budget. Since most systems and networks are not connected to the Internet, existing crisis management measures are run manually and focus on the implementation of information management systems (daily data backups) to ensure business continuity.

NCSS draft states that The Gambia would set up capabilities on cyber crisis management. In that line, the Action Plan of the NCSS draft also states certain actions: a contingency plan would be drafted, a contingency organisation would be set up, and test organisation and plan and team training would be set up to coordinate and work closely with the GM-CSIRT.

D 1.5 CYBER DEFENCE

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. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Start-up

The Gambia in its efforts to become a Digital Nation and a modern information society, the NDP 2018-2021 states that "Government will also strive to build local capacity including Cyber Defence Systems and personnel to protect national security."[36]

[33] The Gambia National Disaster Management Agency. Available at http://www.ndma.gm/home/ (Accessed 12/10/2018)
[34] International Disaster Response Law in The Gambia. Available at https://www.ifrc.org/Global/Publications/IDRL/IDRL%20Report%20The%20Gambia.pdf (Accessed 12/10/2018)
[35] Ibid.
[36] See *supra* note 20.

Nothing was said in the CMM review about cyber defence efforts. No evidence of the existence of a national defence policy or strategy. Defence is treated as a State House issue in The Gambia and thus shielded from public debate as a matter of national security.

It seems that in the current government approach, which is reflected in the NDP's components, cyber defence actions and initiatives would become a priority for the country and would eventually be addressed in the national defence policy or strategy, if any. NCSS draft does not address any cyber defence component, but it states that one of the NCSC's subcommittee, specifically the national security subcommittee, would be composed of the Ministry of Defence and the Intelligence agency (State Intelligence Service). At least some discussion and ideas would come up from the subcommittee.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups 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).

Stage: Start-up

It was not possible to obtain a full and clear picture regarding communications redundancy in The Gambia during the CMM review consultation. However, communications redundancy as a broad concept has been considered in The Gambia, resulting in sectoral actions to backup data and established redundant networks in cases of communication breakdown.[37]

Internet redundancy measures taken by telecommunications operators, including ISPs, are at the organisation and business level, but there is nothing coordinated and systematic actions at the national level. Telecommunications operators have existing coordination mechanisms, in an ad-hoc fashion, if an operator experiences Internet service interruption. There is no evidence that PURA, in its capacity of the sectoral regulator, is taking concrete actions to supervise and monitor the resiliency and redundancy of the networks at the national level.

Some participants highlighted the need to ensure uninterrupted functionality of the systems and the zero tolerance of Internet breakdown for telecommunications operators and ISPs.

[37] PURA Annual Report 2010. Available at http://www.pura.gm/wp-content/uploads/2018/01/Annual-Report_2010.pdf (Accessed 12/10/2018)

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of The Gambia. These recommendations 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 specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 Conduct a national cyber risk assessment in order to revise and update the existing NCSS draft and its Action Plan to ensure that their content not only addresses the baseline components but also reflects the current national needs and priorities of The Gambia in the cybersecurity realm.

R1.2 Encourage the participation of the multi-stakeholders not only in the NCSS draft review process, if occurs, but also in the promotion, implementation and review process of the strategic objective of the final NCSS.

R1.3 Encourage to set out a NCSS review procedure to ensure that the resources allocated to accomplish the strategic objectives are being utilised properly and that the strategic objectives are accomplished in a timely manner. Similarly, collect and evaluate relevant metrics, monitoring processes and data in order to inform decision-making.

R1.4 Ensure that the final NCSS is aligned with other national priorities, strategies and plans to avoid duplication of efforts and misuse of resources.

R1.5 Allocate a reasonable budget to ensure the effective implementation and review of the strategic objectives of the final NCSS.

R1.6 Conduct regular and real-time cyber exercises that provide a concurrent picture of the national cyber resilience.

R1.7 Create the national cybersecurity coordination bodies (NCSA and NCSC) to ensure the effective implementation of the strategic objective of the final NCSS.

INCIDENT RESPONSE

R1.8 Develop an operational central registry, possibly hosted by GM-CSIRT, to categorise and record national-level cyber adverse incidents.

R1.9 Work towards the establishment of the GM-CSIRT to ensure that the technological, financial and human resources are adequate and set up clear processes and defined roles and responsibilities.

R1.10 Establish metrics to monitor and evaluate the effectiveness of GM-CSIRT and establish regular training for the employees of GM-CSIRT and design metrics to assess the result of this training.

R1.11 Create a mandate for a national cyber incident response detailing when and how organisations should report incidents.

R1.12 Improve incident identification and analysis in response and conduct regular systematic updates to the national level incident registry.

R1.13 Promote coordinated national incident response between the public and private sectors, with lines of communications prepared for times crisis.

R1.14 Develop a culture of risk assessment and management predictive methods to assess risk, its propagation and its aggregation for the national and CI domains.

R1.15 Establish mechanisms for regional and international cooperation for incident response between organisations to resolve incidents as they occur.

R1.16 Establish and promote a platform for the reporting and sharing of incidents across sectors.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.17 Develop or make official the list of NCI and NCII sectors, including critical assets and services, stated in the NCSS draft with identified risk-based priorities.

R1.18 Establish a mechanism for regular vulnerability disclosure and information sharing between CI assets owner, operators and government.

R1.19 Establish regular dialogue between tactical and executive strategic levels regarding cyber risks practices and encourage communication among CI operators, operator and government.

R1.20 Establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an incident response plan for cyber adverse incidents.

R1.21 Identify internal and external CI communication strategies with clear points of contact.

R1.22 Establish common processes and procedures to assess and measure the capability of CI assets owner and operators to detect, identify, respond to and recover from cyber threats.

R1.23 Develop a regulatory framework -covering both legal and technical components- concerning NCII by amending the existing legislation or enacting new regulations as needed to encompass incident prevention, detection and response.

R1.24 Allocating an adequate budget for conducting emergency response scenario exercises at a national level, at least once a year.

CRISIS MANAGEMENT

R1.25 Allocate cybersecurity exercise planning to relevant authorities, such as NDMA and GM-CSIRT.

R1.26 Design, implement and test a cybersecurity needs assessment framework to gauge the mitigation measures, protocols and techniques for crisis management. Highly recommendable the involvement of key stakeholders and other experts, such as thank thanks, academic and civil society leaders should be sought.

R1.27 Develop a national business continuity / disaster recovery / contingency plan with the cybersecurity component.

R1.28 Organise national cybersecurity exercises. Since multiple national emergency exercises already exist in the Gambia, it might be more feasible to integrate the cybersecurity component in one of these scenarios. Plan the exercises by engaging relevant stakeholders, outlining their role in the exercise.

R1.29 Identify metrics to evaluate the success of the exercises. Evaluate the exercises and feed the findings back into the decision-making process.

CYBER DEFENCE

R1.30 Develop or ensure that the existing draft or official National Security Strategy takes into consideration not only the cyber defence component but also the identified threats to national security that might emerge from cyberspace. Moreover, ensure that such strategy complies with national and international rules of engagement in cyberspace.

R1.31 Designate an organisation within the Gambian army to host and manage the central command and control of cyber defence capabilities. Establish cyber operation units in different branches of government and armed force as appropriate.

R1.32 Develop a communication and coordination framework for cyber defence, build on existing security structures

R1.33 Expand coordination in response to malicious attacks on military information systems and national critical infrastructure.

R1.34 Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.

R1.35 Establish training programmes for employees and develop awareness campaigns.

COMMUNICATIONS REDUNDANCY

R1.36 Allocate appropriate resources not only to activities, such as hardware integration, technology stress testing, personnel training and crisis simulation drills, but also to ensure that the redundancy efforts are appropriately communicated to relevant stakeholders.

R1.37 Establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response assets communications and authority links.

R1.38 Hardwire all emergency response assets into a national emergency communication network.

R1.39 Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of redundant communications protocols tailored to the roles and responsibilities of each organisation in the emergency response plan.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including users. The days in which cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. 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 programmes for users – systems that can be used easily and be incorporated in everyday practices online.

This dimension reviews important elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This dimension also entails the existence mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D 2.1 CYBERSECURITY MIND-SET

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. 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

When reviewing the cybersecurity mind-set in the Gambia, the review looked at three groups of actors: government, the private sector, and society-at-large.

Participants noted that general awareness for cybersecurity within government agencies was very low. However, participants noted that the level of awareness varies across hierarchical levels: whereas the IT departments and those employees with responsibilities regarding cybersecurity have already developed some cybersecurity mind-set, there has been a lack of awareness for the risks and threats at the highest levels of government and areas not charged with cybersecurity responsibilities.

As an illustration, participants raised concerns over the routine use of private emails by staff across government and public institutions for official correspondence. There was also a consensus that the lack of web literacy, carelessness and ignorance added to such problems as people sharing passwords with colleagues and friends, and saving sensitive files on flash drives.

Participants also agreed that the cybersecurity mind-set in the private sector was similar to that of the public sector. There are some leading banks and e-commerce entrepreneurs that are more aware of cybersecurity issues than other private sector actors, but these organizations represent the minority.

Across society-at-large, a cybersecurity mind-set is emerging among selected groups within academia and civil society. However, there is not yet an engrained cybersecurity mind-set across society. This is partially due to a lack of awareness raising efforts and also because Internet access is still very limited in most regions of Gambia.

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Stage: Start-up

During the review, there was a general consensus among participants that trust in online services relates closely to the level of cybersecurity awareness in the country.

In general, too many Internet users in the Gambia have blind trust in websites and to what they receive from the Internet, especially through social media.

E-government services have yet to be established in the Gambia. It has been noted that the development of those e-government services has been in the process for so long that it is undermining citizens' trust in the ability of the Government to securely and reliably provide such services. Participants have also mentioned a general reluctance of public sector employees in using any government-offered service such as email, due to perceived privacy concerns.

The state of e-commerce services is currently embryonic in Gambia. The range of available e-commerce services is still very limited, and such services are used by a narrow segment of the population. The lack of resilient identification and a street addressing system as well as the lack of a dispute resolution mechanism have been identified as key obstacles to the greater uptake of e-commerce services.

In addition, there is no active effort from the Internet Service Providers (ISP) nor the E-Commerce operators in promoting trust in online services.

E-banking services are still very new to Gambia and despite notable success of mobile payment services, most payments are still done in cash.

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Start-up

Awareness around the protection of personal information and the security of personal data is generally low.

Participants estimated that only a limited number of Internet users are aware of personal data issues and employ good cybersecurity practices when using social media and online services. As most internet users too blindly trust the Internet, personal information is often shared through social media, in particular Facebook.

Licensed Internet service providers are officially required to store, process and use the PII of their customers with due care. In addition, such information could only be shared upon presentation of the appropriate legal requests.

Outside of the telecommunications (and related) services no concrete action or general policy has been put in place to protect user personal information. Also, there has been limited discussion regarding protection of personal information and the required balance between security and privacy in Gambia.

2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning as channels for users to report internet related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Start-up

No central dedicated mechanism exists to enable citizens to report computer-related, online incidents or crimes in Gambia.

PURA does provide a hotline to report issues and dispute with telecommunications operators, but participants did not believe such a hotline would be the right channel to report cybercrime incidents, in particular for hacking incidents. The National police also have established a hotline but is not equipped to handle cyber-related incidents.

D 2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Start-up

In Gambia, cybersecurity issues are insufficiently reported in media both online and offline. Most participants never come across cybersecurity news, either on TV, national press, or social media. For the few who witnessed some reporting about a cybersecurity incident or awareness event, such reporting was taking place in the case of a major international event.

There was a consensus that media and social media should play a major role in raising cybersecurity awareness.

RECOMMENDATIONS

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

CYBERSECURITY MIND-SET

R2.1 Enhance efforts in leading government agencies to promote an understanding of cyber risks and threats and to prioritise cybersecurity.

R2.2 Design coordinated cybersecurity awareness training programmes for employees in the public organisations in a position of leadership.

R2.3 Design online programmes and training materials (e.g. cybersecurity best practices, cyber threat landscape in the Gambia, risk management), in consultation with the civil society and the academia, and make it available freely for the public to help them be safe on their everyday use of the Internet and online services.

R2.4 Promote the sharing of information on incidents and best practices among organisations and across sectors to foster a proactive cybersecurity mind-set.

TRUST AND CONFIDENCE ON THE INTERNET

R2.5 Promote the need for Internet users to critically assess what they see and receive online and to protect themselves when online through awareness and training campaigns.

R2.6 Promote, in collaboration with civil society, the secure use of internet based on indicators of website legitimacy through awareness campaign.

R2.7 Encourage ISPs to establish programmes that promote trust in their services based on measures of effectiveness of these programmes.

R2.8 When introducing e-government services for citizens, implement security measures from the beginning and have them certified by third parties to build trust by citizens.

R2.9 When introducing e-government services for citizens, promote their use through developing an effective communication strategy/plan that focuses on convenience, security and privacy protection.

R2.10 Encourage E-commerce service providers to develop and implement programs informing users of the utility of deployed security solutions and to enhance trust to online services.

R2.11 Encourage the private sector, in particular telecommunication and ecommerce services to employ cybersecurity good (proactive) practices.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.12 Promote the implementation of user-consent policies by Internet operators.

R2.13 Develop programmes in cooperation with civil society and other stakeholders to support existing efforts to raise user awareness about online risks.

R2.14 Promote measures to protect privacy and enable users to make informed decisions when and how they share their personal information online.

R2.15 Encourage public debate on social media platforms and in traditional media regarding the protection of personal information and about the balance between security and privacy to inform policymaking.

R2.16 Develop a Code of Practice on Protecting Personal Information Online that can be distributed to citizens.

REPORTING MECHANISMS

R2.17 Set up a cybercrime "report centre" where the public would be able to report cybercrimes including online fraud, bullying, child abuse online, identify theft, security breaches, and other incidents by dialling a number in case it is an emergency, completing an online form or sending an email.

R2.18 Provide manuals to educate the public about the types of cybercrime that can be reported, how to exercise their rights when falling victim to such crimes and how to report it.

R2.19 Cooperate with the private sector to raise awareness about new and existing reporting channels among the wider public and across stakeholder groups.

R2.20 Consider establishing secure two-way information sharing between the cybercrime report centre and investigators such as the police force.

MEDIA AND SOCIAL MEDIA

R2.21 In cooperation with civil society and media organisations, organize campaigns to raise awareness, for instance, during a dedicated Safer Internet Day/week or the Cybersecurity Awareness Week/Month etc.

R2.22 Enhance the understanding of cybersecurity among media providers and leading social media actors, (e.g. journalists and editors) through tailored awareness campaigns and trainings.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D 3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Start-up

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. Due to the lack of a national awareness programme, cybersecurity awareness amongst the general public is low.

The need for awareness raising programmes has been recognized by the government in the draft national cybersecurity strategy (NCSS), however the final NCSS draft was not officially adopted yet. It has not been updated since 2016 nor submitted for Cabinet´s approval. (see D1.1.) One of the strategic priorities of the NCSS is to raise public awareness on cyber risks and solutions (Section 5.1.4) as part of the national cybersecurity capacity-building efforts in order to prevent cybercrimes such as direct users of e-services to use the most secure solutions. This will be achieved 'by addressing cyber-related topics at all levels of education and informing people based on research and analysis of secure behaviours.'[38] Participants mentioned that there will be a national budget dedicated to awareness and cybersecurity

[38] The Gambia National Cybersecurity Strategy (2016) Draft V1.6. 13 June 2016.

education programmes that will be implemented by the National Cybersecurity Committee (NSC) in 2019.

The Gambia Cyber Security Alliance (GCSA) – a civil society organization with a view to promote, advocate and create awareness on cyber security - conducts cybersecurity awareness campaign and seminars for officials and the general public. [39] The Alliance is also active at the school level, conducts school and community outreach at the grassroots level in order to talk to users about safety online. For instance, in November 2018 the Alliance conducted a community outreach in Busumbala and Essau (North Bank Region) to discuss issues related to social media and society, cybersecurity, internet morals and ethics, mobile phones usage.[40] Also, in July 2018 GCSA in collaboration with PURA organised a three-day training on cybersecurity measures, cybercrime and online bullying for students and civil societies. [41]

Focus-group discussions suggest that awareness of cybersecurity issues is very limited among executive managers both in public and private sectors, which could be one of the reasons why cybersecurity awareness-raising has not yet been perceived as a priority. There was a general consensus among the participants that executives, company managers are not aware of their responsibilities in relation to cybersecurity and do not have a clear understanding of the implications of cybersecurity. Participants recognised the need to raise the cybersecurity awareness of executive staff within the corresponding organisations.

D 3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Start-up

The need for enhancing cybersecurity education in schools and universities has been identified by leading government and academic stakeholders. One of the strategic priorities of the draft NCSC is to ensure the next generation of cybersecurity professionals (Section 5.1.1) though the development of school curriculums concerning cybersecurity:

> Support will be given to raise the number of students having completed a training curricula in cyber security and specific actions will be taken to include women into the cyber workforce. A public-private partnership taskforce on cyber security education will be set up which will focus on giving advice about the cyber security curriculum, in

[39] Gambia Cyber Security Alliance. Available at http://gamcybersecurityalliance.com/ (Accessed 12/12/2018)
[40] Gambia Cyber Security Alliance. GCSA cybersecurity awareness community awareness in Busumbala. Available at http://gamcybersecurityalliance.com/category/latest-news/ (Accessed 12/12/2018)
[41] Ibid.

> relation to the certification of information security experts and the further development of learning modules, among other things. Cybersecurity-specific courses should then gradually be created in universities syllabus.
>
> *(Section 5.1.1. of The Gambia National Cybersecurity Strategy (2016) Draft V1.6)*

It was not clear from the focus-group discussions how these objectives will be prioritized in the implementation of the strategy since currently, there is no national budget to reach the goals.

There is currently no formal cybersecurity education/national curriculum for cybersecurity in The Gambia. Participants confirmed that there is no formal cybersecurity education at the primary or secondary school level. The country has very limited options for cybersecurity qualifications and there is a shortage of qualified cybersecurity educators to improve the situation. The trainings are organised ad-hoc that are mostly self-organized activities run by the GCSA and the International Information System Security Certification Consortium (ISC) focusing on children. Participants' commentary suggested that there are limited sources and tools available for students to practice what they were taught and to make use of their knowledge.

In terms of higher education, the American International University West Africa offers Bachelors of Science Degree in Computer Science & Technology, plus any of Microsoft, Oracle, Cisco, (ISC)² & MOS Certifications.[42] However, there are no elective or mandatory cybersecurity-specific courses offered. There was no evidence of competitions for students. Also, there was a consensus among participants about the need for scholarships in order to make ICT education at postgraduate and doctoral level affordable; currently it is very expensive, costs 20 000 GBP.

Similarly, it was not clear from the focus-group discussions to what extent cooperation between the private sector and the university exists.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Stage: Start-up

The need for training professionals in cybersecurity has been recognized by the government. One of the strategic priorities of the draft NCSC is to provide awareness, training and

[42] American International University West Africa. Computer Science & Technology. Available at http://www.aiu.edu.gm/cmit/computer-science-and-technology.html Accessed 12/12/2018)

education for all stakeholders under Section 3.5 (users and providers of cybersecurity services, experts within institutions in charge of cybersecurity and fight against cybercrime). According to the draft strategy, the National Cybersecurity Authority (NCSA) and a National Cybersecurity Committee (NCSC) will be tasked to organize the governance and implementation of the Strategy. However, focus-group discussions failed to confirm if any distinct budget to reach these goals exists.

No cybersecurity framework for certification and accreditation of public-sector professionals exists. Civil society organisations such as GCSA provides ad-hoc cybersecurity professional trainings to police force and the private sector (i.e. banks) to build a culture of cybersecurity. One participants noted that at the American International University West Africa there are 30 students currently undergoing certification program (technical in orientation, targeting purely ICT professionals) to prepare for jobs in private sector. However, there is a need for professional training and certification offerings both in the public and private sectors.

Metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings do not yet exist. Some participants highlighted the challenges of monitoring the implementation of training and the difficulty to assess if training has filtered down to the grassroots level. Another concern during the review was about the poor conditions to provide trainings in rural areas. For instance, GCSA was planning to conduct training for 50 police officers in a rural area, however there was no infrastructure in place and trainees had to be transported to central locations that resulted in making logistics complicated and the training more expensive. Participants' commentary suggested that there are insufficient technical resources (for e.g. tools and equipment) available to implement lessons learned in trainings.

Also, no employer incentives for employees to participate in trainings seem to exist. Employees that receive training (from external service providers that approach CI operators) might have an informal debrief with colleagues or step up when the occasion to leverage their training arises but would not commonly train colleagues on what they learned. Trainings at times might just focus on preparing participants for exams rather than actually training them on subject matter. Also, ICT courses still focus on how to set up and manage networks and cybersecurity not a priority component.

The Public Utilities Regulatory Authority (PURA) partnered with CISCO to provide cybersecurity specific training with online participation mostly for CCNA and CCNP certificates; however, none of which are specifically geared towards ICT security.

Participants suggested that there is a high demand for cybersecurity professionals; to cover not only the technical aspects but also the behavioural components of cybersecurity. Participants agreed that there is a lack of experts that could offer cybersecurity courses at the scale needed to meet institutional demand for ICT security professionals. Government bureaucracies still set up ICT infrastructure without prioritizing or giving much consideration to network security.

The CMM review did not reveal if a national approach to cybersecurity workforce development or job creation initiatives are a priority to ensure that training offerings exist for cybersecurity professionals through both public and private sources and that organisations are encouraged to establish a cadre of professionals.

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 Gambia. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

AWARENESS RAISING

R3.1 Speed up the acceptance of the draft national cybersecurity strategy in order to advance the development and implementation of a national cybersecurity awareness-raising programme.

R3.2 Confirm the National Cybersecurity Committee, as the dedicated organisation which has the mandate to develop and implement a national cybersecurity awareness-raising programme that would focus on the most vulnerable users, such as children and women, based on international good practice. Coordinate and cooperate with key stakeholders, for instance through a dedicated cybersecurity awareness month, in particular including those who participated in the review (private sector, civil society and international partners).

R3.3 Create a single online portal (for e.g.: on the Ministry's website or on Facebook) linking to appropriate cybersecurity information and disseminate materials for various target groups via the cybersecurity awareness programme and social media.

R3.4 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors as this group is usually the final arbiters on investment into security.

R3.5 Consider establishing a Cybersecurity Academy or a National Cybersecurity Department that centralises cybersecurity awareness training at the national level. Avoid duplication of efforts with the National Cybersecurity Committee.

R3.6 Speed up the Awareness aspects as contained in Strategic Goal 1 "Develop and enhance awareness, training and education" of the draft national cybersecurity strategy (specifically action item 5.1.4 "Rising public awareness on cyber risks and solutions").

R3.7 Integrate cybersecurity awareness-raising efforts into ICT literacy courses (for e.g.: using the computer and managing files, internet and email, concepts of IT) and initiatives at schools and universities that could provide established vehicles for cybersecurity awareness-raising campaigns.

R3.8 Assign the National Cybersecurity Committee to establish metrics and ensure that evidence of application and lessons learnt feed into existing and new developed programmes.

FRAMEWORK FOR EDUCATION

R3.9 Assign an institution (for e.g.: Ministry for Basic & Secondary Education and the Ministry of Higher Education) to develop a national curriculum on cybersecurity-related courses and requirements/standards. Establish institutional guidance to coordinate efforts and leverage resources to greatest effect with regards to ICT policy, ICT curriculum and teaching capacity.

R3.10 MOICI should dedicate a national budget for coordinating cybersecurity education and research.

R3.11 Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators to ensure that skilled staff is available to teach newly formed (and existing) cybersecurity courses.

R3.12 Integrate specialised cybersecurity courses in all computer science degrees at universities and offer specialised cybersecurity courses in universities and other bodies.

R3.13 Make an introductory course in Cybersecurity Awareness a component of ALL University courses.

R3.14 Collect and evaluate feedback from existing students for further development and enhancement of cybersecurity course offerings.

R3.15 Create cybersecurity education programmes for non-IT specialists and make them available at universities and other bodies in the public sector.

R3.16 Design specific cybersecurity programmes at the Bachelor or Master levels. Also, consider hosting annual cybersecurity competitions for students.

R3.17 Investigate the job market in cybersecurity and emphasize and advance the creation of more job opportunities.

R3.18 Consider introducing more technical/ICT related courses at high school level in order to initiate students early-on to spark an interest in the field of cybersecurty and give them a head-start before they begin studies at university.

R3.19 Cybersecurity courses taught at Gambian universities should include ICT/computer lab components during which students can gain practical training and experience managing cybersecurity-related issues.

R3.20 Offer university scholarships or bursaries in order to make ICT education at postgraduate and doctoral level affordable.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.21 Work collaboratively with stakeholders from higher education, private, public-sector and CI to develop an Industry Based Learning programme for students. This programme should be part of the qualification offered and enable: students to gain practical experience in cybersecurity practice and use of technology in participating organisations; organisations to provide feedback; and students to discuss lessons learnt. Use feedback and lessons learnt to revise course content and design to meet current and emerging requirements.

R3.22 Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals. Cooperate with the GM-CSIRT once established; private sector; education; public-sector; CI stakeholders; and international partners to develop those offerings.

R3.23 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.

R3.24 Prioritise funding for professional training of: the national CERT team once established; CI organisations; and other organisations that risk assessments have identified as critical for national interest.

R3.25 Measure and evaluate professional training and take-up, including a feedback mechanism for specialist and organisations to drive further development and enhancement of professional training (e.g.: seminars, online resources, and certification offerings).

R3.26 Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

R3.27 Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals.

R3.28 Document national training needs so that the professional needs of society can be adequately met.

R3.29 Establish regular mandatory training for IT employees and general employees regarding cybersecurity issues.

R3.30 Create specific measures to help government and companies to retain skilled cybersecurity staff.

R3.31 Create a framework for cybersecurity certification and accreditation for public and private sector professionals.

R3.32 Consider investigating the provision of more affordable cybersecurity courses.

R3.33 Ensure that a national budget is made available to the NCSA and the NCSC to implement the strategy.

R3.34 Improve cybersecurity training conditions, including infrastructure (tools and equipment) in rural areas.

R3.35 Emphasize the importance of behavioural content in cybersecurity courses.

R3.36 Increase the number of experts which can offer courses in cybersecurity.

R3.37 Ensure that (cyber) security is integral to the creation of new ICT infrastructures by the government.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Start-up

The Information Communication Act (ICA), which was enacted back in 2009, is the current legal framework governing cyber issues in The Gambia. Such law addresses not only the rapidly evolving nature of the communications industry but also the convergence of technologies.[43] In specific, ICA governs privacy protection and personal data processing, computer misuse and cybercrime, children's protection, e-signature, e-transactions, e-government services, among others, which would be addressed below as part of the legal and regulatory framework review.

During the CMM review, participants indicated that The Gambia requires a more comprehensive framework to address and tackle issues related to cybercrime -substantive and procedural provisions-, ICT security -critical infrastructure (NCII) - and cybersecurity governance, and not just cybercrime. Some participants also stated that the current cybercrime provisions of the ICA have been amended on a piecemeal basis; however, it is time to conduct a profound review to adapt the cybercrime provisions to the current cybercrime

[43] Cybercrime & Cybersecurity Trends in Africa 2016. Available at https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf (Accessed 12/10/2018)

landscape, which has dramatically changed since ICA's enactment, and to incorporate new cyber-criminal offenses, such as fraudulently remaining in a computer system and criminal association.

According to government's representatives, a major law reform is under development on cybercrime so a new legal framework, including substantive and procedural provisions on cybercrime and other cyber-related issues, is expected to be enacted in 2019.

Such cybercrime law reform has been discussed in The Gambia for a while. In fact, as part of the NCSS drafting process and other related initiatives, a proposal for legal implementation was also developed back in 2016 which is, in essence, a draft of legislation for the implementation of the NCSS and its Action Plan. In that sense, NCSS draft contains some actions related to the development of a substantive and procedural law on cybercrime, such as i-) to review of the existing legislation to clearly define all criminal offenses related to ICT, 2-) to define effective, proportionate and dissuasive penalties, and iii-) to enact procedural rules to enable judicial authorities to conduct specific investigation proceedings for cybercrime.

Such proposal of law includes new provisions which are not included in the ICA, such as i-) protection of national critical information infrastructures -definitions, identification of NCI and NCII, and operators' obligations-, ii-) cybersecurity governance/institutional framework -national cybersecurity coordinator, committees and CM-CSIRT, and their roles and responsibilities-, iii-) rules of procedures -search and seizure, data presentation, competent authorities-, iv-) international cooperation -assistance for evidence gathering, designation of point of contact and extradition, and also amendments to some specific provisions which should be more specific. As to cybercrime provisions, specifically, those provisions regarding offences related to ICT, were drafted based on the model provided by the African Union Convention on Cybersecurity and Personal Data Protection[44] (Malabo Convention) which has not been ratified by The Gambia,[45] and the ECOWAS directive on fighting cybercrime.[46]

Nothing was said in the CMM review whether such proposal of law would be adopted as an amendment to ICA or as a separate cybersecurity act. In fact, some participants commented that the Gambian government should consider implementing a different law model, such as the information and communication act and the cybercrime act in Nigeria which are two separate laws. In a recent report, this issue was also addressed and the author concluded that "[ICA] included several relevant e-legislations which needed stand-alone and detailed legislation on their own such as the e-transactions, e-signature and cybercrime legislation. Therefore, there is a need to update and separately develop these important e-legislations."[47]

[44] African Union Convention on Cyber security and Personal Data Protection. Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Accessed 12/10/2018)
[45] African Union Convention on Cyber security and Personal Data Protection – List of members. Available at https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_2.pdf (Accessed 12/10/2018)
[46] ECOWAS Directive. Available at http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf (Accessed 12/10/2018)
[47] Review of the Legal and Regulatory Framework in the Information and Communications Technology Sector in a subset of African Countries. Available at https://www.uneca.org/sites/default/files/PublicationFiles/review_of_the_legal_and_regulatory_framework.pdf (Accessed 12/10/2018)

Despite United Nations' resolution that "the same rights people have offline must be protected online,"[48] digital rights and freedoms are still restricted in some countries, including The Gambia, in which surveillance and monitoring, censorship, criminalisation of online content and the shutting down of Internet have suppressed Gambians' digital rights and freedoms in the past, especially under the previous regime.

While The Gambia has not adopted specific legislation on human rights online, it is a signatory to international instruments on human rights, such as the African Chapter on Human and People's Rights (Banjul Chapter)[49] and other international and regional treaties.[50] According to the Human Rights Report 2017 provided by the U.S. Department of State "[d]uring the year the government did not restrict or disrupt access to the internet or censor online content, and there were no credible reports that the government monitored private online communications without appropriate legal authority."[51] Some process is shown since the new administration took control.

The Constitution of Gambia[52] includes more than twenty provisions regarding fundamental human rights and freedoms, including freedom of speech, conscience, assembly, association and movement (article 25), right to privacy (article 23), right of children (article 29), among others.

Specifically, article 23 of the Gambian Constitution governs privacy as a fundamental right[53] which is subject to certain restrictions in the interest of the national security, public safety, and prevention of disorder o crime, among others.[54] In addition to such constitutional provision, privacy is also ruled by some provisions on the ICA, mainly from the privacy of communications perspective.

According to the Freedom on the Net reports (2016 & 2018), privacy has been a major concern for the Gambians in the last years due to previous regime's policies and laws, including article 138 of ICA which sets out broad and sweeping powers to national security agencies and investigative authorities to monitor, intercept and store communications in unspecified circumstances, such as communications of activists and independent journalists which has also limited their freedom of expression right, while also giving PURA the authority to intrude communications for surveillance purposes without judicial oversight.[55] Moreover, the current legal framework for surveillance conflicts with The Gambia's obligations under international

[48] UNESCO – Internet Universality, ROAM Principles. Available at https://en.unesco.org/news/unesco-welcomes-new-unhrc-resolution-highlighting-online-freedom-expression-and-noting-unesco (Accessed 12/10/2018)
[49] African Chapter on Human and People's Rights. Available at http://www.achpr.org/instruments/achpr/ (Accessed 12/10/2018)
[50] United Nations Human Rights. Treaties ratified by The Gambia. Available at https://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=64&Lang=EN (Accessed 12/10/2018)
[51] U.S. – Country Reports in Human Rights Practices for 2018. Available at https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper (Accessed 12/10/2018)
[52] Constitution of the Republic of The Gambia. Available at https://wipolex.wipo.int/en/text/221243 (Accessed 12/10/2018)
[53] And also article 17 of the International Covenant on Civil and Political Right. Available at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (Accessed 12/10/2018)
[54] Constitution of the Republic of The Gambia. Available at http://hrlibrary.umn.edu/research/gambia-constitution.pdf (Accessed 12/10/2018)
[55] Freedom of Net 2016, The Gambia Profile. Available at https://freedomhouse.org/report/freedom-net/2016/the-gambia and Freedom of Net 2016, The Gambia Profile. Available at https://freedomhouse.org/report/freedom-net/2018/gambia (Accessed 12/10/2018)

and regional human rights laws and treaties to uphold freedom of expression and the right to privacy.[56]

UN Special Rapporteur stated that "... [w]ithout adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistle-blowers, for example, cannot be assured that their communications will not be subject to States' scrutiny".[57] The 2018 report also states that intercepted phone and email communications were often used as evidence in trials against government critics. Government's technical surveillance capabilities remain unknown and it is uncertain whether the new government has continued to carry out the same surveillance practice.[58]

Freedom of speech or expression is governed by article 25 of the Gambian Constitution.[59] Both freedom of expression and privacy are interlinked and mutually dependent so an infringement upon one can also cause severe consequences on the other right. As stated above, freedom of speech was also severely restricted under the previous regime; however, in 2017 the new government announced general legal reforms aiming to strengthen individual freedoms[60] and a public commitment to respect and uphold the human rights of every person.[61]

In 2017, the new Attorney General and Minister of Justice acknowledged before the Supreme Court that Sedition -a law that had been frequently used to silence journalists and critics under the previous regime- was unconstitutional.[62] Furthermore, early in 2018, the Court of Justice of ECOWAS ruled that the Gambian authorities must repeal criminal prohibitions on libel, sedition and false news.[63] In May 2018, the Gambian Supreme Court, in a landmark judgement, declared some provisions of the ICA unconstitutional. Justices struck down criminal defamation, and narrowed the definition of sedition to apply only to "the person of the president" and "administration of justice;" the previous definition included the entire government of The Gambia.[64] As a result of these landmark decisions, the freedom of expression right has been strengthened, especially for journalists, but it still needs to be adequate to international standards.

Not much was said about personal data protection during the CMM review. Gambia has a data protection legal framework which is embedded in the ICA, and which aims to regulate the processing of personal data by telecommunications service providers and to establish provisions to guarantee the confidentiality of the telecommunications. However, ICA's data protection section does not have a general scope, that is, it does not fit for the purposes of protecting personal data since no enshrine the basic principles of personal data that are established in the ECOWAS Supplementary Act on Personal Data Protection (2010), see below, and other international standards.[65]

---

[56] Amnesty International, Human Rights under Threat in Gambia. Available at https://reliefweb.int/sites/reliefweb.int/files/resources/AFR2741382016ENGLISH.PDF (Accessed 12/10/2018)
[57] Ibid.
[58] See *supra* note 55.
[59] See *supra* note 54.
[60] See *supra* note 55.
[61] Sedition Law Unconstitutional. Available at http://foroyaa.gm/sedition-law-unconstitutional-attorney-general/
[62] http://foroyaa.gm/sedition-law-unconstitutional-attorney-general/ (Accessed 08/04/2018)
[63] See *supra* note 55.
[64] Ibid.
[65] International Data Privacy Law. Available at https://academic.oup.com/idpl/article-abstract/7/3/179/4211051 (Accessed 12/10/2018)

Said that, a comprehensive law on personal data protection is a need in the country to ensure that the citizens' personal data is fully protected and also treated in accordance with the international principles and standards. Curiously participants did not point out the need of a comprehensive law, but some participants did mention that the lack of a data protection agency makes very difficult to respond to popular complaints related to data protection concerns and that evidence gathering is also difficult to facilitate prosecution of data protection cases.

ECOWAS Supplementary Act on Personal Data Protection (2010), strongly influenced by the EU Data Protection Directive (95/46/EC), instructed that state members shall establish (i) a legal framework for privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the State (article 1), and (ii) its own data protection Authority which shall be an independent administrative authority responsible for ensuring that personal data is processed in compliance with the provisions of this Supplementary Act (article 14). After almost eight years, neither the general personal data protection law nor the national agency is in place.

Moreover, Chapter II of the Malabo Convention[66] also regulates personal data protection, among other topics, and its main goal in terms of data protection is to establish in each state member a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use. By proposing a type of institutional basis, this convention also guarantees that whatever form of processing is used shall respect the basic freedoms and rights of individuals while also taking into account the prerogatives of states, the rights of local communities and the interests of businesses; and take on board internationally recognized best practices.[67]

Curiously, the NCSS draft does not address any personal data protection component but at least its Action Plan does: "Ministry of Foreign Affairs would be leading the ratification of the Malabo Convention." Changes will not happen overnight so the new administration should include in its cybersecurity agenda the strengthening of the personal data protection component in order to develop a comprehensive legal framework, set up the national data protection agency, and also comply with the international standards and commitments, such as the Malabo convention and said ECOWAS Supplementary Act.

Very little was said regarding child protection online during the CMM review. While The Gambia has not adopted specific legislation on child protection online, it is a signatory to international instruments on child protection, such as the Convention on the Rights of the Child,[68] Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography and other international treaties. Some participants also commented that there is no special legislation for child protection online, but it does exist some general child protection provisions, mainly concerning the distribution of child photographs, which are also set out in the ICA.[69] However, ICA provisions fall short due to article 174 only criminalises the possession of child pornography with the intent to distribute or show, not just mere possession, and

[66] See *supra* note 44.
[67] GCSCC – African Union on Cyber Security and Personal Data Protection. Available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/african-union-convention-cyber-security-and-personal-data-protection-0 (Accessed 12/10/2018)
[68] UN Convention on Rights of the Child. Available at https://www.ohchr.org/en/professionalinterest/pages/crc.aspx. (Accessed 12/10/2018)
[69] Articles 170, 174 and 175 of the ICA

article 164 only criminalises accessing and viewing pornography, not just accessing a computer to distribute, publish or sell child pornography.[70]

The Children's Act 2005 sets out children rights, such as privacy, and prohibits children prostitution, trafficking, etc. which can be brought to the online context as well. Additionally, commercial sexual exploitation of children has become a major concern in the Gambia, and it is frequent that digital components are found in the configuration of this kind of crimes either to advertising sexual tours -website, to contact the minors -social networking sites, instant messaging, or to produce, expose or disseminate illegally material about the minors on Internet -child pornography. In that sense, the Tourism Offenses Act of 2003 also penalises sexual exploitation of children in the Gambia.

As a preventive measure, it is recommended to conduct educational and awareness-raising campaigns focusing on children, parents, teachers, youth organisations and others working groups to enhance their understanding of the child risks on using Internet or mobile phones and other new technologies, including information for children on how to protect themselves, how to get help and to report this kind of incidents.

It is important to highlight that The Gambia definitely requires a comprehensive and effective legislation, in line with international standards, on child protection from all forms of abuse,[71] including online criminal activities – e.g. cyberbullying, grooming-, and also appoint a government agency to oversee all aspect of child protection either online or offline.

The Consumer Protection Act (CPA)[72] came into force in 2014 with the purpose of safeguarding consumers from unfair and misleading market conducts and also ensure that consumer protection rights are guaranteed as well as encouraging fair trade which is geared towards discouraging businesses from engaging in unfair and fraud practices.

CPA is administrated by The Gambia Competition and Consumer Protection Commission (GCCPC),[73] an independent public agency, and enforced by the Consumer Protection Tribunals, which are set in every administrative region of the country. Consumers can lodge their complaints through GCCPC or the Consumer Protection Tribunals which can provide a remedy in the event of a breach of consumer' rights. GCCPC Complaint form (B1) is available online for consumers to describe the facts and submit the claim.[74] Some participants highlighted that the consumer protection field in the Gambia has a higher maturity level than the personal data protection field which does not even have a data protection authority in place.

CPA contains a number of consumer rights, such as the right to privacy, right to choose, right to equality in the consumer market and protection against discriminatory marketing practices, right to disclosure information, right to fair and honest dealing, right to fair, just and

[70] Global Monitoring, Status of Action against Commercial Sexual Exploitation of Children, The Gambia. Available at http://www.ecpat.org/wp-content/uploads/legacy/A4A_V2__AF_GAMBIA_FINAL2.pdf (Accessed 12/10/2018)
[71] The Point Digital Newspaper. Available at http://thepoint.gm/africa/gambia/article/child-protection-specialist-calls-for-stiffer-punishment-for-child-abusers (Accessed 12/10/2018)
[72] The Gambia Consumer Protection Act 2014. Available at http://gcc.gm/gcc/wp-content/uploads/2018/05/GAMBIA-CONSUMER-PROTECTION-ACT-2014.pdf (Accessed 12/10/2018)
[73] Gambia Competition Commission. Available at https://www.consumersinternational.org/members/members/gambia-competition-commission/ (Accessed 12/10/2018)
[74] The Gambia Competition and Consumer Protection Commission. Available at http://gcc.gm/gcc/wp-content/uploads/2018/05/consumer-proctection-complaint-form.pdf (Accessed 12/10/2018).

reasonable terms and conditions, right to fair value, good quality and safety, right to accountability by suppliers, etc.[75]

Gambians buying online are entitled to the same level of protection as with conventional transactions -e.g. privacy, security payment- even though e-commerce in the country is in an incipient stage. While CPA is a relatively new act but has no specific provisions related to online transactions and ICA does regulate electronic transactions (articles 200-211), including consumer protection provisions, this calls on the new government to work with business and consumer groups to identify the new risks posed by online transactions and also determine if legal changes are required to improve consumer trust in e-commerce.

In 2018, a Gambian published in the Point, a local digital newspaper, the following statement "… having the [CPA] in place is indeed a laudable initiative but certainly not good enough without its full implementation as that failure cost the government … [t]he Gambia Consumer Competitive Protection Commission (GCCPC) should also be more effective and proactive in the discharge of the responsibilities they are empowered ... [p]romoting fair competition is indeed a very important element and principle of procurement but ultimately most serve the interest of the consumers."[76]

Early in 2018, GCCPC, in collaboration with the Chamber of Commerce and Industry, launched the Consumer Protection Business Compliance Guide, indeed a great initiative;[77] however, these guidelines are not available in the GCCPC's official website for consumers' consultation. In 2018, GCCPC, in collaboration with PURA and the U.S. Federal Trade Commission, organized a three-day conference called "Protecting Every Consumer in a Digital Age" in which African consumer protection and competition agencies, experts, civil society, and other relevant stakeholders discussed and evaluated the effectiveness of policies, existing laws, cross-border cooperation, share best practices, enforcement approaches and better means to protect consumers in the digital world.[78]

Very little was said about the intellectual property during the CMM review. The Gambia has made some progress in aligning its industrial property regulations with the international standards. Participants stated that while there are general intellectual property (IP) laws in place (Industrial Property Act 2007, Industrial Property Regulations 2010 and Copying Act 2004), and the country is also a signatory to international conventions (Paris Convention, Bern Convention, ARIPO, WTO), there is no specific Legislation applicable to online IP matters and services, and no evidence that provisions of that nature are not being discussed in the Gambia. According to the report "Investment Climate Statements for 2016", The Gambia has not been

[75] Know your Rights – The Gambia. Available at https://allafrica.com/stories/201811020278.html (Accessed 12/10/2018)
[76] The Point Digital Newspaper. Available at http://thepoint.gm/africa/gambia/article/opinion-consumer-welfare-in-the-gambia (Accessed 12/10/2018)
[77] GCCPC, GCCI Launch Consumer Protection Business Compliance Guide. Available at https://allafrica.com/stories/201810170456.html (Accessed 12/10/2018)
[78] The Gambia Competition and Consumer Protection Commission. Available at http://gcc.gm/gcc/the-gambia-competition-and-consumer-protection-commission-hosted-the-9th-annually-african-consumer-protection-dialogue-conference/ (Accessed 12/10//2018)

ratified the World Intellectual Property Organisation (WIPO) Internet Treaties (Copy Right Treaty and Performances and Phonogram Treaties)[79] on Intellectual Property.[80]

In 2018, the Ministry of Justice, in partnership with WIPO, organized a validation workshop for the National Intellectual Property Policy for The Gambia,[81] but such policy is not available for consultation to find out if it is considering any IP protection online measure. The Ministry of Justice, in collaboration with the Gambia Police Force, established an Anti-Intellectual Property Crime Unit at the Police Headquarters in Banjul.[82]

As stated above, The Gambia currently has substantive cybercrime provisions which are set out in the ICA. Since 2016 a cybercrime legislation containing substantive and procedural provisions has been drafted, but not approved yet. It is expected that such cybercrime framework be enacted next year. Moreover, The Gambia has not ratified the Malabo Convention, which covers cybersecurity and personal data protection, and the Budapest Convention, which covers substantive and procedural provisions and international cooperation mechanisms.

Early in 2018, stakeholders in the ICT, security and legal sectors got together, as part of the Council of Europe's capacity building workshop on cybercrime, and acknowledged about the need of enacting robust legal provisions on cybercrime and electronic evidence. Overall, The Gambia has reached important advances to fight against cybercrime and according to government's representative next year, the enactment of the cybercrime legislation and the establishment of the national CSIRT would take the Gambia into a higher maturity level from the cybersecurity perspective.

D 4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Start-up

Across the criminal justice system, capacities are at initial stages of development in the country and also very little was said in the CMM review.

[79] WIPO Internet Treaties. Available at https://www.wipo.int/copyright/en/activities/internet_treaties.html (Accessed 12/10/2018)
[80] U.S. Department of State. Available at https://www.state.gov/e/eb/rls/othr/ics/2016investmentclimatestatements/index.htm#wrapper (Accessed 12/10/2018)
[81] The Point Digital Newspaper. Available at http://thepoint.gm/africa/gambia/article/national-intellectual-property-policy-developed (Accessed 12/10/2018)
[82] WIPO, Trade Policy Review. Available at https://www.wto.org/english/tratop_e/tpr_e/s365_e.pdf (Accessed 12/10/2018).

For more than two decades, the judicial system in The Gambia suffered from neglect, under-investment, and a severe lack of resources and infrastructure, resulting from a general deprioritisation of its importance.[83] The Gambia was also characterized by a disregard for the rule of law, infringements of civil liberties and the existence of a repressive State apparatus.[84] Former leader brought the judiciary to its knees during his tenure, compelling "mercenary judges" to hand down controversial verdicts in court cases suspected to be politically motivated.[85] With the new administration, the judicial system has shown some important improvement, including two landmark court decisions regarding the protection of human rights, and aims at strengthening the country's democratic standards.

Law enforcement agency performs an essential role in achieving the Gambia's cybersecurity objectives by investigating a wide range of cybercrimes. The Gambia Policy Force (GPF) is the primary law enforcement agency which, in collaboration with the U.S. government, Interpol, and other international organisations, has been training law enforcement officers.[86] However, there is not an organised cybercrime unit within GPF, but within the State Intelligent Service exist a cybercrime unit with limited capacity.

According to the NCSS' Action Plan, Ministry of Justice, in collaboration with MOICI, GM-CSIRT and INTERPOL, would set up a specialised law enforcement team to exclusively address cybercrime issues. In that line, the first step would be to identify prosecutors and investigators with skills or interest in this domain and enhance their technical and procedural skills and experience interacting with the GM-CSIRT's experts and also receiving cybercrime training abroad. Additionally, cybercrime, digital investigation and electronic evidence courses would be incorporated within the curriculum on law enforcement.

According to participants, cybercrime training for law enforcement do exist, and multiple countries and international organisations invest resources to build cybercrime capacities in The Gambia; however, trained officers often return from clinics, seminars or conferences, and there is not a support structure in their working environment to operationalise their new knowledge. This kind of training has been given to Gambian law enforcement officers for the last decade, at least one or two events per year, but very little improvement has been reached at the organisational and national level. Some cybercrime training still remains at a baseline level, no specialised or advanced topics, such as digital forensic training, are addressed.

Furthermore, MOICI, as the government ICT development governance agency, and the government of Taiwan entered into a collaboration agreement to set up a digital forensic lab called Taiwan Digital Opportunity Centre (TDOC). This initiative was intended to act as the initial state to raise Gambia Government IT related capability, achieving seamless internal transition when planning for and implementing government IT systems in the future.[87]

[83] International Bar Association. Available https://www.ibanet.org/Document/Default.aspx?DocumentUid=214e3622-85cf-4219-a151-4194a506a204 (Accessed 12/10/2018)

[84] U.N. Report of the Special Rapporteur. Available at https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A_HRC_29_37_Add_2_FRE.DOCX (Accessed 12/10/2018)

[85] Rule of Law at Work in the New Gambia. Available at https://www.freedomnewspaper.com/2018/08/11/rule-of-law-at-work-in-new-gambia/ (Accessed 12/10/2018)

[86] U.S. Embassy in The Gambia Facebook page. Available at https://www.facebook.com/U.S.EmbassyBanjul/photos/a.10150634223410531/10154594712160531/?type=1&theater and https://www.newtimes.co.rw/section/read/193799 (Accessed 12/10/2018)

[87] MOICI. Available at https://moici.gov.gm/tdoc (Accessed 12/10/2018)

However, as a result of a new diplomatic affairs policy that took place in 2016, The Gambia decided to suspend diplomatic relations with Taiwan and re-establish relations with China. Therefore, the resources for the TDOC initiative were also suspended and the TDOC project was never finished.[88]

Some participants also said that if such digital forensic lab initiative is ever retaken, it should be based within the GPF, with the assistance of PURA. GPF currently has a building for this purpose, but no action to actually set it up. Participants commented that the lack of the capacity of the police in investigating cybercrime is mainly related to lack of resources, and this situation also sets back the possibilities of the judicial system to process cybercrime offenses in the country. Participants also commented that GPF and Ministry of Justice should partner up to ensure that digital evidence is properly collected to build a solid prosecution.

In The Gambia, the cybercrime cases which finally get to court are not prosecuted or processed by specialised courts nor prosecutors, they are processed by conventional courts, judges and prosecutors who may have a certain level of expertise or training in cybercrime. According to some participants, the courts assign cybercrime cases to judges based on his/her level of expertise in this domain. Not many judges and prosecutors have such expertise on cybercrime.

Some participants commented that the lack of coordination within the Judicial System causes that prosecutors or judges who have been trained on cybercrime, then are moved to other departments or positions wasting the training effects and misusing the financial and human resources.

Participants also stated that most of the cybercrime offences that have been brought to court are related to government's loss of revenue. Such cybercrime offenses have been prosecuted on the basis of economic crimes and also procedures for conventional offenses are being applied due to the lack of procedural provisions on cybercrime. As a result of this situation, the investigation and prosecution of many cybercrime cases are delayed and sometimes hampered. According to some participants gathering and preserving digital evidence is always a procedural issue due to the current documentary evidence law, enacted back in 1994, has not been revised to reflect the technological advances. When digital evidence is in hands of ISPs, law enforcement always contacts ISPs directly to get access to user data, and the formal request has to come from Criminal Investigation Department (CID) at the Police Headquarters. Some participants manifested that there are some concerns about the fact that law enforcement agencies approach ISPs directly to access information without obtaining a court order beforehand.

Some participants with legal background also stated that substantive cybercrime law needs to be accompanied by procedural rules, such as provisions for gathering and preserving digital evidence, since admissibility of evidence is key to carry out a successful investigation and prosecution of cybercrime offences. Moreover, other laws and legal provisions, such as the e-transaction provisions, rely on a robust cybercrime legislation.

[88] Gambia president tells China previous Taiwan ties a "huge mistake". Available at https://af.reuters.com/article/topNews/idAFKCN1LM1P4-OZATP (Accessed 12/10/2018).

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Stage: Formative

The Gambian authorities have recognised the need to improve informal and formal cooperation mechanisms, both domestically and across borders, but in general terms, these mechanisms remain ad-hoc.

When GM-CSIRT begins operations, supposedly early in 2019, information sharing mechanisms at the national and international level should be deployed in an organized and efficient manner. It would also help to coordinate better the existing domestic and international cooperation initiatives, and to avoid duplication of efforts and maximize the limited resources.

At the international level, The Gambia has not ratified both the Budapest Convention which contains an entire chapter for international cooperation mechanisms and assistances. The Gambia has been working closely with Council of Europe, ECOWAS, the Commonwealth and Interpol to enhance the domestic cybercrime legislation and set up collaboration mechanisms at a regional level.

Some participants stated that in 2018 the government of The Gambia and Interpol reached a MoU on sharing cybercrime information. Moreover, Interpol's West Africa Police Information System (WAPIS) is an initiative to create national criminal data systems, including cybercrime issues, in each country of ECOWAS. Such systems together would create a regional platform for stronger criminal data sharing enabling the region's police to better tackle crime challenges through improved data sharing. The Police's cybercrime database, once set up, could be shared partially with the domestic judicial system and other ECOWAS countries.

The NCSS' Action Plan states that The Gambia would take actions to promote an active international cooperation on cybersecurity, including the following actions: setting out liaison with regional CERTs and IMPACT for sharing experiences, skills and operational information on cybersecurity, considering the possibility to become a member of FIRST, identifying and participating in regional and transregional forums on cybersecurity. Additionally, setting out liaison with regional law enforcement agencies for sharing understanding, experience, skills and judicial information on cybercrime, identifying and participating in regional and transregional forums and training on cybercrime, considering the ratification of the Malabo Convention and the ECOWAS Convention on Extradition, and identifying other legal instruments to both request and assist other countries related to cybercrime matters, e.g. bilateral agreements, international legal frameworks and mutual legal assistance.

At the national level, government agencies, law enforcement and private sector are sharing information in an ad-doc manner. They do not follow any international protocols (e.g. traffic light protocol) or best practices to disclose sensible or confidential information among them.

Cooperation between government and criminal justice actors, informal relationships have been established successfully, mostly based on personal connections, resulting in the exchange of information on cybercrime issues.

Cooperation between law enforcement and the private sector, in particular ISPs, is informal, as there are no legislative requirements for information sharing between domestic public and private sectors. When law enforcement agencies require access to information held by ISPs or any other regulated operator, PURA has set out an informal procedure to process the data access requirement. Basically, the "formal" request is sent from the Police Headquarters to ISPs, and law enforcement officer's ID needs to be attached at the request of the operator, so in case of any complaint on data mishandling or misuse, ISPs can track down who requested access to the information.

Regarding cooperation between civil society and law enforcement, some participants stated that civil society actors have been organizing training and seminars for law enforcement, but Police Headquarters does not send technically-minded officers, so hands-on training has turned out inefficient. Participant from law enforcement suggested setting up new participation requirements to really take advantage of this training.

Some participants suggested setting up a cybersecurity committee in the National Assembly (currently there is an ICT committee) and also adding MOICI to the ICT committee which was created a decade ago when ICT security concerns did not feature prominently on the security agenda.

Some participants said that there must be a national reporting mechanism in place to keep track and report all cyber-related incidents that occur in The Gambia, including cybercrime event, and that this task should be handled by the GM-CSIRT or the GPF Cybercrime Unit when set up. Other participants stated that some sectors have made some important progress on this, for instance, the financial sector has a focal body called the Financial Intelligence Unit.

According to some government's representatives, ISPs and other telecommunications operators are obligated to report cyber incidents, of any nature whatsoever to PURA because they are licensed operators which own and operate communication infrastructure. There is not a specific provision on the ICA but it is deemed an implicit obligation that is deduced from the license agreements. Therefore, IPSs and telecommunications operators must report any adverse incidents, including cyber incidents, to PURA. Some participants stated that issues related to critical infrastructures would be reported to a hotline managed by PURA.

Also, cyber-bullying offences are rarely reported because victims feel uncomfortable to come forward due to the bullying complaint must be filled in person. According to some participants, The Gambia should borrow the Nigerian model which allows filling the complaint either through a hotline or in person.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to The Gambia. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL FRAMEWORKS

R4.1 Review the existing legal and regulatory mechanisms for ICT security to identify where gaps and overlaps may exist and amend or enact new laws accordingly.

R4.2 Ensure that international and regional trends and best practices inform the assessment and amendment of domestic legal frameworks protection human rights online and associated resources planning. In order to meet dynamic changes in the application of technology to human rights, identify procedures to amend and update legal frameworks as needed. Ensure such legal framework also meets The Gambia's international commitments (e.g. treaties, conventions).

R4.3 Ensure that a comprehensive personal data protection law is successfully enacted and implemented in accordance with the international and regional standards and best practices and that legal mechanisms are in place that enable its enforcement, including the establishment of a data protection agency.

R4.4 Ensure that a national child protection online law is successfully enacted and implemented in accordance with international and regional standards and best practices that legal mechanisms are in place that enable its enforcement, including the establishment of a coordination and monitoring agency.

R4.5 Ensure the development and implementation of specific provisions and procedures on the current or new consumer protection legal framework in order to meet the international standards and best practices in the application of technology to the consumer protection.

R4.6 Ensure that an intellectual property protection online law is successfully enacted and implemented in accordance with the international standards and best practices.

R4.7 Review the existing cybercrime legal framework to incorporate not only new cybercrime offences but also procedural provisions to investigate, prosecute and process domestic and cross-border cybercriminal activities in accordance with the international and regional standards and best practices.

R4.8 Review and implement specific legal provision on e-commerce concerning cybercrime incidents, such as online fraud, spam, and phishing sites.

R4.9 Considering developing a separate strategy covering cybercrime specifically that would also clarify the roles and responsibilities of the actors (GM-CSIRT, cybersecurity coordination agencies, law enforcement, government agencies and institutions) involved in handling computer security incident response and cybercrime investigations.

R4.10 Considering developing a platform for sharing electronic evidence between regional and cybercrime forces.

R4.11 Establish formal and adequate procedures, protocols, and provisions to enhance the cooperation between ISPs and law enforcement agencies. Revise and enforce legal or administrative provisions that obligate ISPs to provide technical assistance to law enforcement when conducting cybercrime investigations.

R4.12 Considering ratify and implementing international, regional and national cybercrime instruments, including the Budapest and Malabo conventions.

R4.13 Allocation of sufficient financial and human resources to accomplish the national priorities to fight against cybercrime.

CRIMINAL JUSTICE SYSTEM

R4.14 Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of law enforcement officers and investigators.

R4.15 Allocate resources dedicated to full operational cybercrime unit(s) based on strategic decision-making in order to support investigations, especially at the local level.

R4.16 Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.

R4.17 Develop and institutionalise specialised training programmes for law enforcement officers, including police, prosecutors and judges on cybercrime, electronic evidence and personal data protection matters. Additional resources should be allocated for this specific purpose. Consider establishing standards for training of law enforcement officers on cybercrime.

R4.18 Establish a specialised cybercrime unit within the GPF to be the central point of contact to carry out cybercrime investigations both domestically and internationally.

R4.19 Build a cadre of specialised prosecutors and judges on cybercrime and electronic evidence to investigate, prosecute and process cybercrime-related cases.

R4.20 Establish formal mechanisms, protocols and best practices to enable not only information sharing but also cooperation between prosecutors and judges in order to ensure efficient and effective prosecution.

R4.21 Collect and analyse statistics and trends regularly on cybercrime investigations, prosecutions and convictions.

R4.22 Consider requesting accurate and updated cybercrime statistics from coordination agencies (NCSA and NCSC), GM-CSIRT, PURA and MOICI in order to better inform decision-makers about the current cybercrime threat landscape in The Gambia when developing policies and legislation.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.23 Establish formal international cooperation mechanisms to combat cybercrime based on existing legal assistance frameworks, mutual legal assistance and extradition provisions, and further bilateral and international agreements (e.g. Budapest Convention).

R4.24 Facilitate informal cooperation mechanisms within the law enforcement and criminal justice system, and between law enforcement and third parties, both domestically and cross-border, in particular ISPs. Consider know-hows from other areas, such as anti-corruption cooperation.

R4.25 Allocate resources to support information sharing between the public and private sectors at the national level and enhance the legislative framework and communication mechanisms, protocols and standards.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-up

There is currently no coordinated effort to develop a nationally agreed baseline of cybersecurity related standards and good practices in the Gambia.

Generally, Banks and Financial institutions are further advanced in applying cybersecurity standards, as they are under obligations determined by international bodies such as PCI SSC and Swift.

There is also no mechanism to establish synergies between government and the private sector to harmonise approaches towards cybersecurity standards implementation.

Participants also agreed that no cybersecurity standards or good practices have been implemented to guide the procurement process or software development within the public sector. No such practice has been implemented in the private sector either.

D 5.2 INTERNET INFRASTRUCTURE RESILIENCE

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Start-up

Participants raised several concerns regarding the resilience of Internet infrastructure in the Gambia. Even though Internet infrastructure is continuously expanding, Internet penetration is limited, and service is not yet reliable.

Participants emphasized the need to make the national backbone more resilient as Gambia relies on one single submarine cable for access to the Internet, the backup being a much lower capacity terrestrial cable connection to Senegal.

D 5.3 SOFTWARE QUALITY

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Start-up

Policies on software deployment, maintenance and update are not common in the Gambia. Software quality is not monitored and there is no catalogue of secure software. Participants noted that the use of counterfeit or unlicensed software was a common practice in the Gambia.

Several participant from the private sector also advised the top priority for companies when acquiring a software would be the basic functionality and the price, software quality and security requirements being secondary concerns.

Overall, the diversity of software available across the Gambia was perceived as an obstacle to effective monitoring and quality assessment.

D 5.4 TECHNICAL SECURITY CONTROLS

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Stage: Start-up

The use of technical security controls in the Gambia varies across sectors and organisations. While the use of firewalls to protect networks is a common practice for banks and ISPs, the use of technical security controls is very inconsistent across the rest of the private sector as well as in the public sector.

ISPs also advised that while they try to protect their networks, they do not yet offer anti-malware software or other technical security solutions to their customer and do not encourage users to take proactive measures to secure their personal devices.

As for basic Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS), they are rarely deployed.

In general, the level of understanding and deployment of security controls by public and private sectors appears to be low in the Gambia.

D 5.5 CRYPTOGRAPHIC CONTROLS

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.

Stage: Start-up

Participants stated that the need for encryption was recognized, but that the implementation has not yet commenced for most of them. Within the telecommunications and financial sectors, data are routinely encrypted in transit.

The capacity to deploy cryptographic controls is still very low across sectors.

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-up

The domestic market for cybersecurity technologies and cybercrime insurance products has not yet been developed in the Gambia. While international providers offer a range of cybersecurity products for domestic use such as firewall, there are no domestic commercial cybersecurity products or cybercrime insurance offerings.

D 5.7 RESPONSIBLE DISCLOSURE

This factor explores the establishment of a responsible-disclosure framework for the receipt and dissemination of vulnerability information across sectors and, if there is sufficient capacity, to continuously review and update this framework.

Stage: Start-up

No responsible disclosure policy or framework has been established in the public or private sectors. Vulnerabilities are perceived as confidential commercially valuable information and, as such, organisations prioritise solving detected issues internally and do not share information as they don't feel compelled to do so.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity Standards, Organisations, and Technologies, the following set of recommendations are provided to The Gambia.These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1 Establish a program to identify, adapt and/or adopt international information risk management standards applicable to government agencies, personal and/or ICT infrastructure, solutions.

R5.2 Promote adoption of international IT and cybersecurity standards for procurement.

R5.3 Promote the adoption of relevant standards in software development in coordination with different professional communities such as IT professionals, academia and private sector.

R5.4 Promote adoption and implementation of international IT and cybersecurity standards among private sector companies.

INTERNET INFRASTRUCTURE RESILIENCE

R5.5 Enhance coordination regarding resilience of Internet infrastructure across public and private sectors and expand the national program for infrastructure development.

R5.6 Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.

SOFTWARE QUALITY

R5.7 Develop a catalogue of secure software platforms and applications within the public and private sectors.

R5.8 Develop policies and processes on software updates and maintenance that applicable across all government institutions and encourage private sector to do so.

R5.9 In partnership with academia and civil society, gather and assess evidence of software quality deficiencies and it impact on usability and performance for the country and use the result to raise awareness within both public and private sector.

TECHNICAL SECURITY CONTROLS

R5.10 Promote development of repositories of up-to-date technical security controls in both public and private sector.

R5.11 Promote professional (private and public sector) and user understanding of the importance of anti-malware software and network firewalls.

R5.12 Promote professional (private and public sector) and user understanding of the importance of deploying Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS.

R5.13 Encourage ISPs to establish policies for technical security control deployment as part of their services.

CRYPTOGRAPHIC CONTROLS

R5.14 Encourage the development and dissemination of cryptographic controls across all sectors for protection of data at rest and in transit, according to international standards and guidelines.

R5.15 Encourage Web service providers to deploy state of art tools such as SSL and TLS to protect communications between servers and browsers as part of their standard packages.

R5.16 Raise public awareness of secure communication services, such as encrypted/signed emails.

CYBERSECURITY MARKETPLACE

R5.17 Extend collaboration with the private sector and academia and incentivise them in investing in of cybersecurity technological research and development.

R5.18 Work with key stakeholders to assess the financial risk of cybersecurity breaches or crimes for the public and the private sector and encourage the development of specific cyber insurance products.

R5.19 Promote sharing of information and best practices among organisations, to explore potential cybercrime insurance coverage.

RESPONSIBLE DISCLOSURE

R5.20 Develop a responsible vulnerability disclosure framework within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledge report.

R5.21 Encourage sharing of technical details of vulnerabilities among critical infrastructure managers/operators.

R5.22 Incentivise public and private sector entities to provide adequate training and certification programmes to their professionals so that they can identify and address bug and vulnerabilities in their systems.

ADDITIONAL REFLECTIONS

Even though the level of stakeholder engagement in the review was more limited than we might have hoped, which limits the completeness of evidence in some areas, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 29th country review that we have supported directly.

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

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity