DIGITAL DEVELOPMENT PARTNERSHIP

CYBERSECURITY CAPACITY REVIEW

Cape Verde

October 2019

WORLD BANK GROUP

WITH SUPPORT FROM:

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Mr Bonyaminou Porrogho, Mr Samba Mbaye

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

Approved by:

Version	*Date*	*Notes*
1	*12/17/2019*	*Original version submitted to the TechBoard*
2		

LIST OF ABBREVIATIONS

ANAC	National Communication Agency
CCNA	Certified Cisco Network Associate
CCNP	Certified Cisco Network Professional
CIP	Communication Infrastructure Policy
CID	Criminal Investigation Department
CIRT	Computer Incident Response Team
CMM	Cybersecurity Capacity Maturity Model for Nations
CNI	Critical National Infrastructure
CSIRT	Computer Security Incident Response Team
ECDV	Digital Strategy for Cape Verde
ECOWAS	Economic Community of West African States
GCSCC	Global Cyber Security Capacity Centre
HIDS	Host Intrusion Detection Systems
ICT	Information and Communication Technologies
IGO	Intergovernmental Organisation
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunications Union
IXP	Internet Exchange Point
NCS	National Cybersecurity Strategy
NDMA	National Disaster Management Agency
NDP	National Development Plan
NGO	Non-Governmental Organisation
NIDS	Network Intrusion Detection systems
NIST	National Institute of Standards and Technology
NOSi	Nucleo Operacional da Sociedade de Informacao
PII	Personal Identification Information
PKI	Public Key Infrastructure

SME	Small and medium-size Enterprise
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UNCITRAL	Unite Nations Commission on International Trade Law
WACS	West African Cable system
WB	World Bank
WTO	World Trade Organization

EXECUTIVE SUMMARY

The World Bank Group undertook a review of the maturity of cybersecurity capacity in Cape Verde at the invitation of National Security Advisor's office. The objective of this review was to enable Cape Verde to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period 23-25 September 2019, 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) and the banking sector as well as international partners. Telecommunication companies have not attended the critical infrastructure session but had had a chance to meet with a representative of the team during a pre-assessment visit.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model for Nations (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 contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping together related *indicators*, which 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 Cape Verde 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

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

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.

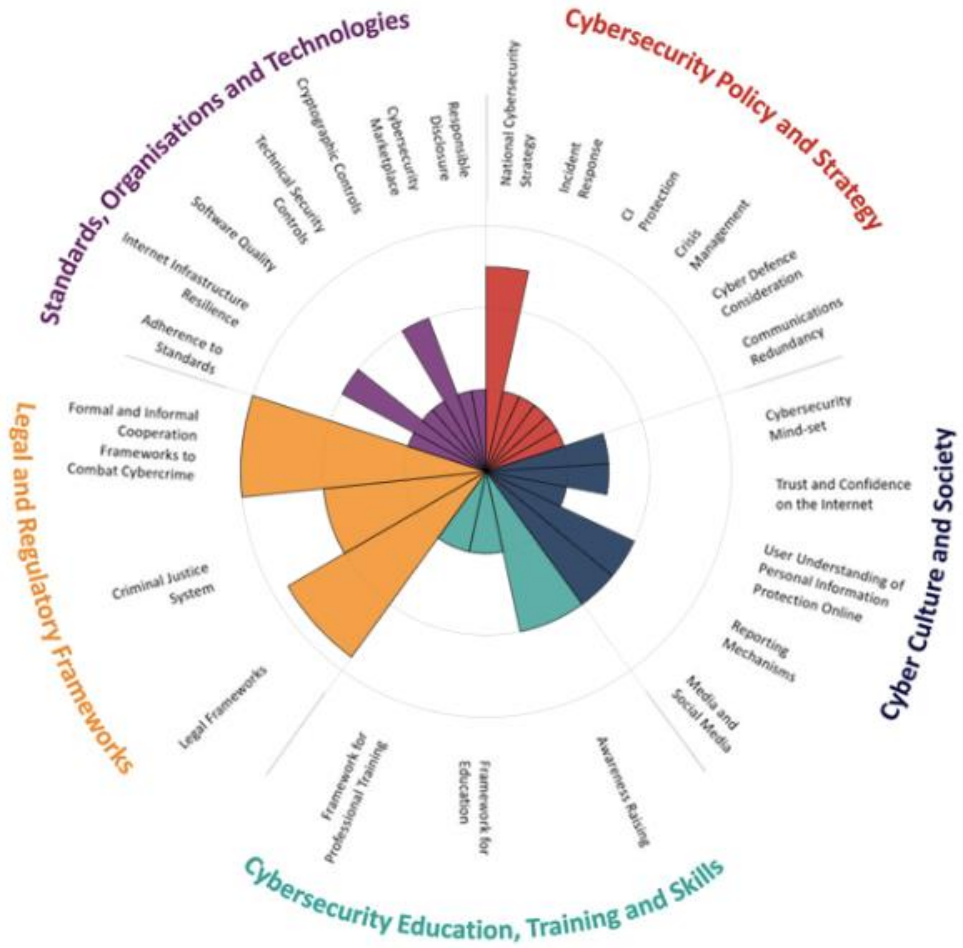

Figure 1: Overall representation of the cybersecurity capacity in Cape Verde

Cybersecurity Policy and Strategy

The consultations have indicated that the national capacity of Cape Verde for the cybersecurity policy and strategy dimension was at Start-Up to Formative level of maturity.

The national cybersecurity strategy for Cape Verde, Estrategia Nacional para a Ciberseguranca[2], was formally approved and published in March 2016. The strategy aims to set national cybersecurity guidelines between 2016-2020. According to CMM review participants, not many actions have been taken since the adoption of the national strategy. However, since the turn of 2019, government officials have started taking steps towards implementing the national cybersecurity strategy. In April 2019, they created a National Council for Cybersecurity.

Currently, Cape Verde does not have a national cybersecurity incident response plan, or a mechanism for early alert of cybersecurity incidents. Additionally, there is no centralised registry for cybersecurity incidents. Some participants from the banking and telecommunications sectors stated that they had developed internal incident response procedures.

Cape Verde does not have a critical infrastructure protection framework and has not yet identified the critical national infrastructure. According to government representatives, a regulatory risk management framework for critical infrastructure will be established as part of the implementation of the NCS. At the time of the CMM review, cybersecurity crisis management did not exist in Cape Verde. Per the NCS, the National Council for Cybersecurity will be responsible for cybersecurity crisis management.

There is no national cyber defence strategy in Cape Verde. Army representatives advised that they have been working closely with their counterparts in the European Union, Ghana, and Portugal to build capacity before they start drafting the defence strategy. According to the NCS, a national cyber defence strategy will be developed.

Cyber Culture and Society

Overall, the cybersecurity culture and society dimension of Burkina Faso is assessed as being at a Start-up to Formative level of maturity.

When reviewing the cybersecurity mind-set in Cape Verde, the review looked at three groups of actors: government, private sector, and society-at-large. Participants agreed that general awareness of cybersecurity varies across hierarchical levels of the government: whereas employees with responsibilities regarding cybersecurity might have developed aspects of a cybersecurity mind-set, this characteristic does not extend to broader groupings within governmental institutions.

[2] CMM review team and World Bank consultants had access to the electronic version of the national cybersecurity strategy for Cape Verde.

During the review, there was a 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 Cape Verde have blind trust in what they receive from the Internet, primarily through social media. E-government services are well developed in Cape Verde, and include most public sector activities such as taxes, administration, transportation, education, health, etc.

Awareness around the protection of personal information and the security of personal data in Cape Verde is generally low. Participants estimated that only a limited number of Internet users are aware of personal data issues and consciously employ good cybersecurity practices when using social media and online services.

Internet-related crimes are to be reported to various entities. For example, online fraud and identity theft would be reported to the national or the judiciary police in person or by telephone. Privacy issues are to be reported to the Data Protection Commission in person. There is limited coverage of cybersecurity issues in media both online and offline. Most reporting takes place in cases of major international events or incidents. Major national cybercrime issues also get some coverage, but as in the case of international incidents, limited information is provided.

Cybersecurity Education, Training and Skills

Overall, the cybersecurity Education, Training and Skills dimension of Burkina Faso is assessed as being at a Start-up to Formative level of maturity.

Awareness-raising courses and seminars are available for a targeted audience within the public and private sectors, but a national programme for raising awareness of cybersecurity, led by a designated organisation (from any industry) which addresses a wide range of demographics, is yet to be established in Cape Verde. Existing awareness-raising initiatives are mostly aimed toward law enforcement, IT professionals and employees at the leadership position and are organised with international partners

A very limited number of cybersecurity educators are available in Cape Verde, and no formal national curriculum for a cybersecurity degree is currently available. At the time of the assessment, there was no cybersecurity framework for certification and accreditation of cybersecurity professionals within the public or the private sector. Most employees and professionals receive cybersecurity training abroad, as no cybersecurity certification nor training is offered in the country.

Legal and Regulatory Frameworks

The consultations have indicated that the national capacity of Cape Verde in the cybersecurity legal framework dimension was at Formative to Established level of maturity.

Cape Verde updated its legislation in 2017 as part of the Budapest convention ratification process. The new comprehensive ICT legislative and regulatory framework addresses cybersecurity, and also the protection of the rights of individuals and organisations that evolve in the digital environment. Specific legislation includes privacy, data protection, electronic transactions, substantive and procedural criminal law.

According to CMM participants, domestic laws recognise fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association.

General consumer protection legislation, protecting consumers, has been adopted since 1998 with Law No 88/V/98[3]. However, it did not contain provisions that address e-commerce specifically. Therefore, in 2007, law No 46 was enacted to cover all advertising practices, including online advertising. While Cape Verde has not adopted specific legislation on Child Online Protection, article 9 of Law No. 8/IX/2017, on cybercrime, firmly condemns the production, the diffusion, and the broadcasting of child pornography.

Substantive and procedural cybercrime legal provisions are addressed by Law No. 8/IX/2017 on cybercrime and the general criminal law. Cape Verde Parliament adopted Law No. 8/IX/2017 in November 2006, and it entered in effect in March 2017, as part of the Budapest Convention ratification**.** The law covers provisions on the collection of digital evidence, on cybercrime and international cooperation.

It is important to note that, to date, the legislative framework for ICT Security which is critical to make sure all the CNI stakeholders follow minimum requirements as far as cybersecurity is concerned, is still to be developed. For instance, during the CMM review, participants stressed the need for a comprehensive law addressing the protection of critical national infrastructure and the roles and responsibilities of the CNI operators.

All entities of the criminal justice system seem to have been created. According to participants to the CMM consultations, a specialised unit within the judiciary police was created in 2017 and tasked with investigating cybercrimes. This brigade is composed of five members, including three inspectors. Participants believe that, due

[3] http:// adeco.cv.free.fr/Law_consumidor.htm

to limited resources, the brigade is not as effective as it should be. As for the court system, it was reported that some training sessions had been held for some judges and prosecutors, but it is unclear how much of the content was tailored to the local legislation or how many professionals attended.

As part of the ratification of the Budapest convention, Cape Verde has established international, and mostly multilateral formal cooperation mechanisms to combat cybercrime by facilitating its detection, investigation, and prosecution. Examples of cooperation include preservation and disclosure of computer data, access to computer data, and seizure and disclosure of data stored in computer systems located in Cape Verde.

At the national level, Law No. 8/IX/2017 on cybercrime states that the competent authority, on the requisition of the prosecutor or order of the investigating judge, is authorised to collect, record, or maintain by any technical means, data associated with a specific computer system or communication. It can also compel a service provider, within the scope of its existing technological capabilities, to assist in collecting or recording data related to communications within the territory.

Standards, Organisations, and Technologies

Overall, the cybersecurity Standards, Organisations, and Technologies dimension of Burkina Faso is assessed as being at a Start-up to Formative level of maturity.

At the time of the CMM review, no specific cybersecurity-related standards nor framework were adopted for use within the government entities in Cape Verde. Government entities mostly relied on the technical controls implemented by NOSI[4], the entity responsible for operating the government ICT infrastructure. Within the private sector, no cybersecurity standards nor good practices have been promoted, and the adoption of international standards is still very low. Banks and Financial institutions are further advanced in applying cybersecurity standards thanks to contractual obligations such as PCI DSS and the Swift cybersecurity framework

Cape Verde relies on the WACS as the sole submarine cable for accessing the Internet. The EllaLink[5] project, which is a submarine cable linking Brazil and Portugal via Cape Verde, would address the redundancy for Internet connectivity for the country and

[4] https://nosi.cv/index.php/en/nosi/about-us

[5] https://www.globenewswire.com/news-release/2018/12/13/1666520/0/en/Cape-Verde-Telecom-and-EllaLink-sign-agreement-for-connectivity-to-Cape-Verde-on-the-EllaLink-Submarine-Cable-System.html

will also bring an additional 400 Gbps capacity. To connect the islands, a redundant fibre loop has been deployed and is fully operational.

Policies on software development, deployment, maintenance and update are not standard in Cape Verde. Software quality is not monitored, and there is no catalogue of secure software. The use of technical security controls varies across sectors and organisations in Cape Verde. 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 sectors.

Cryptographic controls for protecting data have been recognised by the public sector in Cape Verde. To support the uptake of e-government services, a National Public Key Infrastructure (PKI) has been established and cryptographic based state of the art controls have been implemented within the government infrastructure and platforms. Within the financial sectors, data are routinely encrypted in transit, but the capacity to deploy cryptographic controls is still lacking across sectors.

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.

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 with the notable exception that no participation from the telecommunication sector was recorded. Fortunately, a representative of the review team had met separately with all telecommunication operators and ISPs at an exploratory and pre-assessment visit, and gathered enough information to serve the purpose of this review.

INTRODUCTION

At the invitation of *the office of the National Security Advisor* and in collaboration with the Global Cyber Security Capacity Centre (GCSCC), the World Bank (WB) has conducted a review of cybersecurity capacity of Cape Verde. The objective of this review was to enable Cape Verde to determine areas of capacity in which the government might strategically invest in, in order to improve their national cybersecurity posture.

Over the period 23-25 September 2019, stakeholders from the following sectors participated in a three-day consultation process:

- Public sector entities
- Criminal justice sector
- Finance sector
- Critical infrastructure owners
- Academia
- International community

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM)[6] 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 together with the factors which each present:

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

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

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping together related *indicators*, which 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 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 particular circumstances of the state or organisation.
- **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 Cape Verde 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. For 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.[7] 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.[8] 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.[9]

---

[7] Relevant publications: Williams, M. (2003). *Making Sense of Social Research*. Sage Publications: London; Knodel, J. (1993). "The Design and Analysis of Focus Group Studies: A Practical Approach". in *Successful focus groups: Advancing the state of the art*. Morgan, D. L. (Ed.). SAGE Publications: Thousand Oaks, CA; Krueger, R.A. and Casey, M.A. (2009). *Focus Groups: A Practical Guide for Applied Research*. Sage Publications: London.

[8] Relevant publications: Kitzinger, J. (1994). "The Methodology of Focus Groups: The Importance of Interaction between Research Participants." *Sociology of Health & Illness*, 16(1). Available at https://doi.org/10.1111/1467-9566.ep11347023 (accessed 25 February 2018); Kitzinger, J. (1995). "Qualitative Research: Introducing Focus Groups". *British Medical Journal*, 311(7000). Available at https://doi.org/10.1136/bmj.311.7000.299 (accessed 25 February 2018); Fern, E.F. (1982). "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*, 19(1). Available at https://doi.org/10.1177%2F002224378201900101 (accessed 25 February 2018).

[9] Kitzinger, J. (1995).

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 the data generated by focus groups.[10] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[11]

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.[12] 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.[13] Dey explains that this process categorises data as "belonging together".[14]

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 the data collected by the Centre, 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 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 the Centre's 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

---

[10] Krippendorff, K. (2004). *Content Analysis: An Introduction to its Methodology*. Sage Publications: Thousand Oaks, CA; Hsieh, H.F. and Shannon, S.E. (2005). "Three Approaches to Qualitative Content Analysis*." Qualitative Health Research*, 15(9). Available at https://journals.sagepub.com/doi/pdf/10.1177/1049732305276687 (accessed 25 February 2018); Neuendorf, K.A. (2002). *The Content Analysis Guidebook*. Sage Publications: Thousand Oaks, CA.

[11] Fern, E.F. (1982).

[12] Elo, S. and Kyngäs, H. (2008). "The Qualitative Content Analysis Process." *Journal of Advanced Nursing*, 62(1). Available at https://doi.org/10.1111/j.1365-2648.2007.04569.x (accessed 25 February 2018); H.F. and Shannon, S.E. (2005).

[13] Downe-Wamboldt, B. (1992). "Content Analysis: Method, Applications, and Issues." *Health Care for Women International*, 13(3). Available at https://doi.org/10.1080/07399339209516006 (accessed 25 February 2018).

[14] Dey, I. (1993). *Qualitative Data Analysis: A User-friendly Guide for Social Scientists*. Routledge: London.

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.

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

CYBERSECURITY CONTEXT IN CAPE VERDE

The vision of Cape Verde's Digital Strategy (ECDV)[15] is: "A connected Cape Verde, with itself and with the world, developed, inclusive, democratic, open to the world, modern, safe, where full employment and full freedom prevail". It has articulated three priority pillars, including the expansion of the connectivity infrastructure, the enhancement of capacity building, and the provision of digital services through a regional marketplace.

Multiple projects are currently ongoing to support the vision of the ICT sector, which has resulted in significant growth in the last decade. For instance, The EllaLink[16] project, which is a submarine cable linking Brazil and Portugal via Cape Verde, will address the redundancy for Internet connectivity in Cape Verde given the current reliance on sole WACS infrastructure, and will also bring an additional 400 Gbps capacity. With extra available capacity, the aim will be to significantly reduce Cape Verde's digital divide by providing universal connectivity access within the various islands of the archipelago through public-private partnerships. This will support high-speed connectivity and access to online academic content for higher education institutions and secondary schools, and will enable more adoption of the WebLab programme which seeks to empower the next generation of digital leaders for the government and private sectors.

To reach the connectivity objectives, the government of Cape Verde has also been promoting Public-Private Partnerships and Direct Private Sector Investments in order to stabilise, explore and preserve: (i) the launch of the network "Amílcar Cabral" consisting of fibre optic cables for sub-regional capitals: Nouakchott, Dakar, Banjul, Bissau, Conakry, Freetown and Monrovia (ECOWAS); (ii) the connection to the fibre optic cable PEACE, through South Africa and Mozambique ; (iii) the launch of fibre optic cable DILCE between Cape Verde and the United States (Boston); (iv) the renewal and implementation of "sub-loops" on the network of fibre-optic inter-island; (v) the

[15] https://estrategiadigital.gov.cv/index.php/pt/paad-2?download=3:resumo-executivo-da-estrategia

[16] https://www.globenewswire.com/news-release/2018/12/13/1666520/0/en/Cape-Verde-Telecom-and-EllaLink-sign-agreement-for-connectivity-to-Cape-Verde-on-the-EllaLink-Submarine-Cable-System.html

building the Data Center of Mindelo (DC3); (vi) and the Data Center Expansion Beach (DC2).

Cape Verde has also significantly invested in establishing a world-class data centre at the Technology Park in Praia. With seven levels of security, it hosts and manages data and already provides services to the Government of Cape Verde, companies, banks, national and foreign entities. It is also designed to offer cloud computing services (Cloud services). According to NOSi, only 50% of the data centre's capacity is currently utilised[17].

In addition to connectivity, the government aims to build a Regional ICT HUB in Cape Verde by setting up communication networks that will allow the offering of services such as IP connectivity, cloud services, wholesale international connection to the neighbouring countries, national and regional IXP installation, and Internet "peering".

Internet

The percentage of individuals using the Internet in Cape Verde has significantly grown over the past two decades, with 57.162% adoption in 2017, compared to 0.241% in 1997[18]. According to ITU, there were 3.03 per cent fixed (wired)-broadband subscriptions per 100 inhabitants, compared to 70.01 per cent active mobile-broadband subscriptions per 100 inhabitants[19] in 2017. According to the World Economic Forum's 2017-2018 Global Competitiveness Index report[20], Cape Verde ranks 84th in the world on Technological Readiness (including the availability of latest technologies, mobile and fixed broadband subscriptions, and Internet bandwidth).

Cybersecurity

The Government of Cape Verde approved the National Cybersecurity Strategy in February 2016. The NCS sets priorities and objectives to be achieved by 2020[21]. In April 2019, the commission on Cybercrime was created with representation from different government agencies to lay the foundations to implement the NCS.

Meanwhile and as part of the implementation of the NCS, Cape Verde ratified the Budapest Convention on Oct 1st 2018, after being invited to accede by the Council of

[17] https://www.nosi.cv/index.php/en/services/data-center

[18] https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2017&locations=CV&start=1997

[19] https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&CPV

[20] http://reports.weforum.org/pdf/gci-2017-2018/WEF_GCI_2017_2018_Profile_CPV.pdf

[21] https://www.coe.int/en/web/octopus/-/cape-verde

Europe in September 2017. In addition, the law № 8/IX/2017 covers provisions on the collection of digital evidence, on cybercrime and international cooperation.

REVIEW REPORT

OVERVIEW

This section provides an overall representation of the cybersecurity capacity in Cape Verde. 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.

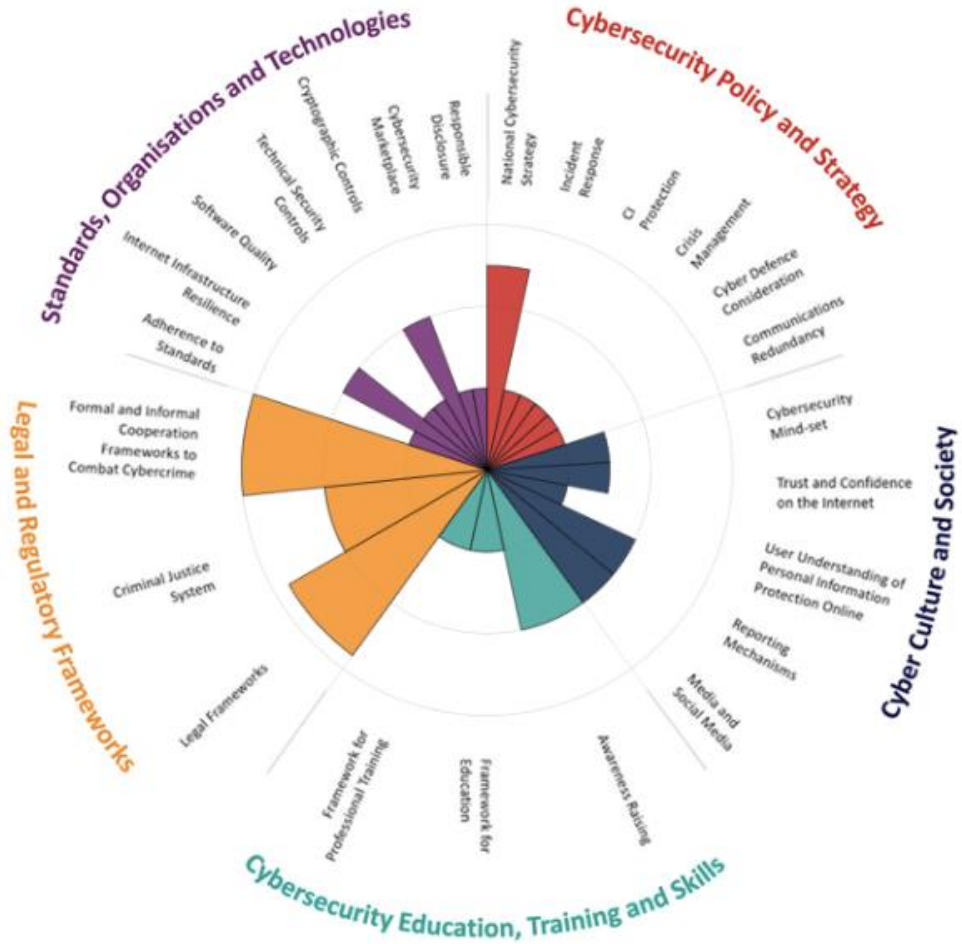

Figure 2: Overall representation of the cybersecurity capacity in Cape Verde

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

The factors in Dimension 1 gauge Cape Verde'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

The national cybersecurity strategy for Cape Verde, Estrategia Nacional para a Ciberseguranca[22], was formally approved and published in March 2016. The strategy aims to set national cybersecurity guidelines between 2016-2020. Most participants of the CMM consultations, specially the ones from the private sector, could not confirm the participation of their companies in the elaboration of the strategy. According to government representatives, this national cybersecurity strategy constitutes an essential pillar of Cape Verde's ECDV.

[22] CMM review team and World Bank consultants had access to the electronic version of the national cybersecurity strategy for Cape Verde.

The approved NCS highlighted the creation and implementation of 5 priority areas, as follow: (i) the creation of legal framework; (ii) the creation of a structure for incident response; (iii) the creation of a Capacity-building structure in cybersecurity; (iv) the development of organisational measures and procedures for risk management; and, (v) the necessary international and diplomatic cooperation. These objectives were defined to effectively improve Cape Verde's capacity to respond to cybersecurity threats. At the time of approval, the National Communications Agency, ANAC[23], was designated to lead the implementation and the monitoring of the major priorities of the national cybersecurity strategy.

According to CMM review participants, not many actions have been taken since the adoption of the national strategy. In fact, the vast majority of the participants in the review were not aware of the existence of the strategy, even though it was published in the official national bulletin. According to government officials, the implementation of the strategy was delayed because a few months after the approval, a new president was inaugurated and a new cabinet installed, leading to a shift in short term priorities. Consequently, many projects, including the implementation of the national cybersecurity strategy, were delayed**.** It is important to highlight that, at the time of the CMM consultations, Cape Verde's NCS did not include an implementation plan.

However, since the turn of 2019, government officials have started taking steps towards implementing the national cybersecurity strategy. In April 2019, they created a National Council for Cybersecurity, chaired by the National Security Advisor with the following core mandates: (i) coordinate the national cybersecurity efforts by streamlining the implementation of the NCS; and, (ii) set up the national cybersecurity centre. At the time of the CMM review, and according to government officials, the commission had a short-term mandate which should end in 2020. However, the commission has submitted a proposal, to the prime minister, aiming to extend the terms of its mandate up to 2024 to allow for full implementation of the strategy. It is important to note that, at the time of the CMM review, the commission was only composed of government officials and members from government agencies.

An area of concern for the participants of the CMM review is the availability of financial resources dedicated to cybersecurity in Cape Verde. According to government representatives, there is no dedicated nor consolidated national budget for cybersecurity. This situation is seen as a potential impediment to the implementation of the NCS.

[23] http://www.anac.cv/

D 1.2 INCIDENT RESPONSE

Stage: Startup

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.

Currently, Cape Verde does not have a national cybersecurity incident response plan, or a mechanism for early alert of cybersecurity incidents. There is also no centralised registry for cybersecurity incidents. Most participants, from both public and private sectors, stated that they have no knowledge of any guidance on how to proceed in case of a cyber incident. Per the national cybersecurity strategy, a coordination body (i.e., the centre) for the reporting and management of cybersecurity incidents will be created.

Some participants from the banking and telecommunications sectors stated that they had developed internal incident response procedures. However, there is no legal requirement in place for them to report cybersecurity incidents. Furthermore, participants confirmed that no communication mechanism to share cybersecurity incidents and/or information among themselves had been implemented.

According to participants of the CMM assessments, the first draft of the structure of the national CSIRT is prepared. This CSIRT will act as the governmental and national operational centre, and will have the mandate to act and react to cybersecurity incidents or threats targeting ICT infrastructure in Cape Verde. Also, the national critical infrastructure operators will be required to report cybersecurity incidents to the CSIRT. During the CMM review, participants could not confirm if the entity responsible for the CSIRT was designated. Per government representatives, the national CSIRT should be operational by January 2020, even though there was no allocated budget at the time of the CMM reviews

According to government representatives, the main functions of the CSIRT will be to provide early warnings, alerts, announcements, and dissemination of information (I) to relevant stakeholders about ICT vulnerabilities, risks and incidents; (ii) to inform the relevant authorities in the event of an incident on an ICT-based systems; (iii) to provide cybersecurity guidance to the national critical infrastructure operators; (iv) to oversee the exchange of information to organise in cyber drills; and, (v) to cooperate with international CSIRT organisations and national CSIRTs.

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

Stage: Startup

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.

Cape Verde does not have a critical infrastructure protection framework and has not yet identified the critical national infrastructure. Government representatives stated that they had identified the national critical infrastructure operators, but at the time of the CMM review, no official communication between them has taken place. There is no vulnerability disclosure among CI owners nor between the government and the CI operators. In addition, none of the CI owners attending the review follows a specific Information security framework in protecting their infrastructure from cybersecurity risks.

According to government representatives, a regulatory risk management framework for critical infrastructure will be established as part of the implementation of the NCS. The legislation will also specify the scope of reporting requirements as well as the vulnerability disclosure among CI operators, and also between the government and the CI owners. It will also define the responsibilities of critical infrastructure operators.

According to participants, cybersecurity risk assessments are not conducted at the national level, mainly because of a lack of incentives. On the other hand, participants from private entities mentioned that, in the past, they had requested the services from a consultancy firm to conduct risk assessments for them. Per the national cybersecurity strategy, a thorough cybersecurity risk management analysis, especially for the critical national infrastructure, will be conducted as part of the implementation process.

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: Startup

At the time of the CMM review, cybersecurity crisis management did not exist in Cape Verde. According to the NCS, the National Council for Cybersecurity will be responsible for cybersecurity crisis management. There are crisis management processes and procedures for national security, but cybersecurity is not included. Government representatives believe that they can adapt their national security management processes and procedures to fit any cyber crisis if and when necessary – however, a cyber crisis management exercise for the country has never been conducted and the extent to which private organisations consider crisis management is unclear.

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: Startup

There is no national cyber defence strategy in Cape Verde. Army representatives advised that they have been working closely with their counterparts in the European Union, Ghana, and Portugal to build capacity before starting to draft their defence strategy.

According to the NCS, a national cyber defence strategy will be developed to focus on the following: (i) elaborate an action plan for National Cyber Defence that includes risk analysis; (ii) create a cybersecurity team in the Armed Forces and train military personnel to understand, prevent and combat cyber threats; (iii) train and technically equip the military to anticipate, analyse and manage cybernetic risks; (iv) train and technically equip military personnel to detect and block attacks on their infrastructure; and, (v) create a Military CSIRT for Defence and National Security. The review did reveal that the armed forces are yet to be made aware of such an assignment/responsibility. The Army representative confirmed that the armed forces were not included in the national cybersecurity council, nor involved in the implementation of the NCS.

During the review, it was mentioned that a programme designed to educate soldiers about the risks of the Internet had just begun. However, participants acknowledged that the programme needs to be refined to be more effective. A few participants

articulated that they need to use different means to reach out to their audience/target. For instance, many believed that they should have open sessions, or use the official paper of the army to raise awareness better.

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: Startup

At the time of the CMM review, Cape Verde was connected to the Internet through the WACS cable**.** A second cable, the Ellalink, was expected within the next 12 months and will provide redundancy of the path to international. This new submarine cable, which will connect Brazil and Portugal via Cape Verde, will bring enhanced resiliency and capacity of Internet access with an additional 400Gbps[24].

According to CMM review participants, there is no coordinated and systematic communication redundancy management at the national level. The assets required to communicate in a time of crisis and to coordinate an adequate response to a largescale cybersecurity incident were not identified to allow for gaps and overlap assessment.

[24] https://www.globenewswire.com/news-release/2018/12/13/1666520/0/en/Cape-Verde-Telecom-and-EllaLink-sign-agreement-for-connectivity-to-Cape-Verde-on-the-EllaLink-Submarine-Cable-System.html

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 Cape Verde. 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 Identify the highest priority actions within the strategy and set clear time-bound objectives and an appropriate budget

R1.2 Ensure that responsibilities of the relevant delivery agencies are clear and that they are accountable to the council.

R1.3 Ensure that the council is supported with a coordinating body with the skills, resources, and authority to monitor progress on the strategy on the council's behalf.

R1.4 Invite private sector and civil society stakeholders to review the resultant strategy and plan – adjust it accordingly.

INCIDENT RESPONSE

R1.5 Establish a national body in charge of cybersecurity incident response (CSIRT) with specific roles and responsibilities, with the right budget and authorities

R1.6 The CSIRT should establish the relationships with relevant private sector entities for both information sharing and incident support.

R1.7 Ensure that the National Cybersecurity Council is able to oversee the CSIRT's work and has visibility of its progress and performance

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

R1.9 Create a mandate for a national cyber incident response detailing when and how organisations should report incidents. Reach consensus among stakeholders on architecture, interfaces, and standards for information exchange.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.10 Conduct a national risk assessment aiming to develop the list of CNI, with identified risk-based priorities.

R1.11 Establish what standard of cybersecurity is required in order to ensure that these sectors meet the minimum level of security and resilience required and put in place incentives on them to reach this level.

R1.12 Establish collaboration mechanisms that allow for effective information sharing, vulnerability disclosure and incident support between these sector bodies and the CSIRT, as well as between CI assets owners, operators and government.

CRISIS MANAGEMENT

R1.13 Consider including how the country would respond to a cybersecurity-related crisis in the existing national crisis management plan.

R1.14 Conduct an exercise programme to test the ability of the national crisis management system to respond to plausible cyber scenarios.

CYBER DEFENCE

R1.15 Conduct a risk assessment to establish the threat to the ability of the CV armed forces to operate within a contested cyber environment

R1.16 Develop a cyber defence strategy and associated action plan to bring these risks to an acceptable level

R1.17 Establish what role (if any) the armed forces should play in protecting wider government and the CNI.

COMMUNICATIONS REDUNDANCY

R1.18 Identify critical communication infrastructure used for emergency and crisis management.

R1.19 Define the level of redundancy needed for the identified communication network used for crisis management.

R1.20 Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet 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 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

Stage: Start-up to Formative

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

Participants agreed that general awareness of cybersecurity varies across hierarchical levels of the government. Whereas the employees with direct responsibilities regarding cybersecurity might have developed aspects of a cybersecurity mind-set, these attitudes, habits and practices are far less prominent in broader contexts within governmental institutions.

Leading government agencies such as NOSi have started identifying risks and threats associated with cyberspace. Furthermore, the adoption of a National Cybersecurity Strategy as well as the creation of the National Council for Cybersecurity tasked to implement the Strategy have been viewed by governmental representatives as a testimony of a growing awareness of risks and threats among those at the highest levels of the government.

As for the private sector, there was a consensus that the overall cybersecurity mind-set was low despite the fact that leading companies within the banking sector have begun identifying high-risk practices and implementing international best practices and standards in managing cybersecurity. In addition, programmes and materials for training and improving cybersecurity practices within the private sector have yet to be created.

Across society-at-large, there is not yet an engrained cybersecurity mind-set. For most citizens, good habits, attitudes, and practices are learned through experience as they fall into traps set by cyber-scammers.

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 to Formative

During the review, there was a 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 Cape Verde have a blind faith in what they receive online, primarily through social media. Participants believed that things have

been evolving in the right direction among the upper-middle-income groups and intellectuals, but much more needs to be done in support of the population at large. In addition, no there is no evidence that operators of internet infrastructure have considered measures to promote user's trust to online services.

E-government services are well developed in Cape Verde and include most public sector activities such as taxes, administration, transportation, education and health. Despite a few outstanding glitches, e-government services are generally trusted and used in Cape Verde. Participants did advise that face-to-face interaction with public servants is still preferred among elderly people and on the smaller islands.

Only a limited portion of Internet users has trust in the security of e-commerce services available in Cape Verde. The range of available e-commerce services is minimal and appears to be limited to online utility bill payment. Participants also alluded to a platform allowing subscribers to order food from local restaurants, with the actual payment being done in cash, on delivery. It also appears that social media, such as Facebook, is being used often to connect sellers and buyers on a large scale; the actual transaction taking place in a face-to-face interaction.

The limited number of potential customers, a lack of awareness, and a perceived lack of trustful dispute resolution mechanism have been identified as critical obstacles to the greater uptake of e-commerce services. A significant lack of trust in electronic payment systems has also been listed as a key factor impeding the greater uptake of e-commerce. According to participants, such distrust might be due to a lack of awareness, but more importantly, to numerous glitches experienced while trying to use available services. For example, participants reported many instances of utility companies challenging payments made online with the consumer having to show proof of payment and other transactions, with no mechanism for recourse or arbitration.

Nevertheless, there appears to have been little or no active effort from the Internet Service Providers (ISP) nor the e-Commerce operators to promote trust in their online services.

With regard to e-banking, the service remains very new to Cape Verde, and most transactions are still based on cash. Unlike the majority of countries in the region, mobile payments are yet to be developed in Cape Verde.

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 in Cape Verde is generally low.

Participants estimated that only a limited number of Internet users are aware of personal data issues. Very few consciously employ good cybersecurity practices when using social media and online services. Most Internet users too blindly trust the Internet, and social media, leading many to share sensitive personal information over social media, such as Facebook.

Licensed Internet service providers are officially required to store, process and use the Personal Identification Information of their customers with due care. In addition, they can only share such information upon presentation of the appropriate legal requests. A Data Protection Commission responsible for enforcing data protection law was established in 2018 as an independent body with a mandate to investigate and reprimand and/or fine companies and individuals breaking the law.

The Commission organises ad-hoc awareness campaigns targeting the general public and also works in partnership with the Department of Education on ad-hoc communication actives targeting schools.

However, the communication activities of the Commission are not part of a comprehensive programme and participants have cited budgetary reasons for the limited scale of the communication outreach. In addition, the Commission has raised technical capacity and human resource issues as impediments to its capacity to efficiently conduct the auditing and investigative work critical to its mandate.

2.4 REPORTING MECHANISMS

Stage: Formative

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.

In Cape Verde, Internet-related crimes are to be reported to various entities. For example, online fraud and identity theft would be reported to the national or the judiciary police in person or by telephone. Privacy issues are to be reported to the Data Protection Commission in person. Incidents related to specific products are to be reported to the service providers such as telecommunications operators, ISPs, utility companies and banks, through various channels.

The communication channels for reporting such events are still not well defined and are not across sectors, localities, nor at a national level. Most importantly, most participants to the review did not have a clear knowledge and/or understanding of those communication channels.

No entity has been designated for the reporting of other cybersecurity incidents such as security breaches.

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: Formative

In Cape Verde, there is limited coverage of cybersecurity issues in the media both online and offline. Most reporting only takes place in cases of major international events or incidents. Major national cybercrime issues also get some coverage, but as in the case of international incidents, limited information is provided.

There was a consensus that media and social media should play a more significant 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 Appoint, task and fund a designated body to have national responsibility for Cybersecurity Awareness.

R2.2 Task the designated body to coordinate cybersecurity awareness efforts and initiatives at a national level with other stakeholders such as academia, civil society, law enforcement, the Data Protection Commission, cybersecurity professionals, etc.

R2.3 Task the designated body to design online programmes and training materials in consultation with civil society and academia, and make it available freely for the public to help improve awareness and good safety practices in their everyday use of the Internet and online services. Topics could include cybersecurity best practices, how to be safe online, cyber threat landscape in Cape Verde, risk management.

R2.4 Task the designated body to build a coalition with academia, civil society and cybersecurity professionals to help the people of Cape Verde improve their awareness and good safety practices in their everyday use of the Internet and online services.

R2.5 Task the designated body to partner with professional corporations/organisations within critical infrastructure sectors such as finance, telecommunications, health, energy and water, to promote an understanding of cyber risks and threats and to prioritise cybersecurity.

R2.6 Task the designated body to promote the sharing of information on incidents and best practices among organisations and across sectors to foster a more proactive cybersecurity mind-set.

TRUST AND CONFIDENCE ON THE INTERNET

R2.7 Task the designated body to promote the need for Internet users to protect themselves and critically assess what they see and receive online, through awareness and training campaigns. Leverage social media as well as traditional media such as community radios, community TV stations and public gatherings, etc.

R2.8 Task the designated body to promote, in collaboration with civil society, the secure use of the Internet-based on indicators of website legitimacy through an awareness campaign. Use various communication channels to advise on the existence of such indicators.

R2.9 Task the designated body to partner with regulator and ISPs to establish programmes that promote trust in their services and include a measurement of programme effectiveness.

R2.10 Task the designated body to partner with the regulators, banks and e-commerce service providers to develop and implement programmes aiming to enhance trust in online services by informing users of the scope and effectiveness of deployed security solutions.

R2.11 Task the designated body to partner with the private sector, in particular, telecommunication and e-commerce services to proactively employ good cybersecurity practices by using government incentives and/or imposing minimum security standards.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.12 Allocate appropriate budget to the Data Protection Commission to create and execute comprehensive programmes promoting measures to protect the privacy of individuals and enable users to make informed decisions when and how they share their personal information online. Coordinate such effort with the national cybersecurity awareness programme.

R2.13 Task the designated body to promote public debate on social media platforms and in traditional media about the protection of personal information and the balance between security and privacy, then use the outcome to inform policymaking.

REPORTING MECHANISMS

R2.14 Task the designated body to set up a centralised cybercrime or cyber incident "report centre" where the public would be able to report cybercrimes or any cybersecurity incident including online fraud, bullying, child abuse online, identify theft, security breaches, and other incidents. Reporting mechanisms would include a toll-free number, an online form, an email address, etc. Such a centre will interact with specialised agencies to assign cases. The Centre could be a new entity or one of the existing agencies.

R2.15 Task the designated body to provide training materials 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.

R2.16 Task the designated body to partner with the private sector, civil society and academia to raise awareness about new and existing reporting channels among the wider public and across stakeholder groups.

R2.17 Consider establishing secure two-way information sharing channels between the cybercrime reporting centre and investigators, such as the cybercrime unit of the police force, and the incident response centre.

MEDIA AND SOCIAL MEDIA

R2.18 Task the designated body to enhance the understanding of cybersecurity among media providers and leading social media actors, (e.g., journalists and editors) through tailored awareness campaigns and training.

R2.19 Task the designated body to partner with civil society and media organisations, organise campaigns to raise awareness, for instance, during a dedicated Safer Internet Day/week or the Cybersecurity Awareness Week/Month, etc.

R2.20 Create a formal communication channel between law enforcement, the incident response centres and the media to allow for timely access to the right information and to improve cooperation between the media and those institutions.

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: Formative

Awareness-raising courses and seminars are available for a targeted audience within the public and private sectors, but a national programme for cybersecurity awareness-raising, led by a designated organisation (from any industry) which addresses a wide range of demographics is yet to be established in Cape Verde.

Existing awareness-raising initiatives are mostly toward law enforcement and IT professionals in leadership positions. These initiatives are organised with international partners and are not yet linked to the national strategy.

The Data Protection Commission organises ad-hoc awareness activities toward the public about privacy and data protection issues, but these are not part of a comprehensive and funded programme and are not linked to the national strategy nor coordinated with other stakeholders involved in cybersecurity matters.

Participants also agreed that most executives in public, private, academic and civil society are made aware of the risks of cybercrime, but not necessarily how cybersecurity threats at large might impact their organisation. Participants recognised the need to raise the cybersecurity awareness of executive staff within the corresponding organisations.

Top executives in the government and leading sectors such as telecommunications and finance are more aware of cybersecurity risks in general and how their organisation deals with cybersecurity issues, but might not have been made aware of strategic implications.

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

A very limited number of cybersecurity educators are available in Cape Verde, and no evidence suggests the existence of a qualification programme for cybersecurity educators at a national level. The university of Cape Verde did report small scale initiative involving three PHD students focusing their dissertation in cybersecurity in Europe.

There is no accreditation for cybersecurity education in Cape Verde. At the University of Cape Verde, some general ICT curriculums have been amended to add cybersecurity topics with a medium-term goal to allow for students to graduate in ICT with some basic knowledge in Cybersecurity. Participants suggested that limited resources and tools are available for students to practice what they were taught and to make use of their knowledge.

The need for enhancing national cybersecurity education was highlighted in both the National Cybersecurity Strategy and the national digital economy development strategy but implementation has not started yet.

A network of national contact points for government, critical industries and education institutions to improve cybersecurity education is yet to be established. Likewise, discussion of how coordinated management of cybersecurity education and research enhances national knowledge development has not yet begun.

There was also no evidence of competitions for students designed to attract talent in cybersecurity or the general ICT field. At the primary and secondary level, there are no cybersecurity topics built into the programmes. However, the country has introduced ICT related topics and training for secondary schools and has initiated the "Web Lab" project aimed at students and young people from 7th to 12th grade. This project is designed to reduce the digital divide and attract youngsters to science and technology fields.

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.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

Stage: Start-up

At the time of the assessment, participants agreed that most employees and IT professionals received cybersecurity training abroad as no cybersecurity certification nor training was offered in the country. There was also a consensus on the lack of experts that could offer such cybersecurity courses at the scale needed to meet institutional demand for ICT security professionals

Even though the NCS recognized the need to outline a plan for such training, the need for training professionals in cybersecurity was not yet documented at a national level.

The CMM review team could not confirm that a national approach to cybersecurity workforce development or job creation initiatives was a priority. Likewise, the review team could not confirm any national effort to ensure an increase of cybersecurity professional training offerings through both public and private sources.

Participants did confirm that NOSI, the ICT operator for government services, has created an incubator through which it provides hands-on training to new ICT graduates. The area of expertise is mainly focused on the traditional ICT field, and to some extent, some cybersecurity areas.

In both private and public sector, training was provided to general IT staff on cybersecurity issues so that they can react to incidents as they occur but no training for dedicated security professionals existed.

Employees that receive training might have an informal debrief with colleagues but would not commonly train colleagues on what they learned.

Despite the lack of formal metrics evaluating the need and the uptake of ad-hoc training courses, seminars, online resources, and certification offerings, participants agreed that there was a need for professional training in cybersecurity.

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 Cape Verde. 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 Appoint, task and fund a dedicated body (for example the Data Protection Commission) with the responsibility for coordinating all cybersecurity awareness efforts by cooperating with all relevant stakeholders such as the banks, law enforcement, academia, civil society and more.

R3.2 Task the dedicated body to prioritise the development and implementation of a national cybersecurity awareness-raising programme as part of the implementation of the National Cybersecurity Strategy. Ensure that international examples inform such awareness-raising programmes.

R3.3 Task the dedicated body to create a national online Cybersecurity Portal and use the Portal and social media to publish appropriate cybersecurity information and disseminate materials for target groups as part of the national Cybersecurity Awareness program.

R3.4 Task the dedicated body to integrate cybersecurity awareness-raising efforts into all courses at schools and universities. Use those courses as vehicles for cybersecurity awareness-raising campaigns.

R3.5 Task the dedicated body (or another more relevant body) to coordinate all existing Cybersecurity Awareness initiatives for Executive Management and to develop and implement new Cybersecurity Awareness courses for Executive Management where needed.

R3.6 Task the dedicated body to establish metrics to determine the success of all the cybersecurity awareness-raising efforts.

FRAMEWORK FOR EDUCATION

R3.7 Assign a dedicated institution (e.g., Ministries of Education) to coordinate all existing cybersecurity curricula for schools and for Universities, and where necessary develop new such curricula based on international best practices.

R3.8 Dedicate a national budget for cybersecurity education and research.

R3.9 Assign a dedicated institution to develop 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.

R3.10 Assign a dedicated institution to integrate specialised cybersecurity courses into all computer science degrees at universities and offer, on longer-term, dedicated cybersecurity curriculums or majors.

R3.11 Assign a dedicated institution together with other relevant stakeholders, to host annual cybersecurity competitions for students at all levels.

R3.12 Task the dedicated institution, together with other relevant stakeholders, to create of cybersecurity-focused incubators and to ensure that cybersecurity Laboratories are created where students can experiment with the theory provided in courses.

R3.13 Offer university scholarships or bursaries to make ICT education at a postgraduate and doctoral level affordable.

R3.14 Task the dedicated institution, together with other relevant stakeholders, to establish metrics to determine the success of all course offerings and to enhance such offerings if needed.

R3.15 **Workforce dev**

R3.13

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.15 Identify and task a dedicated institution or body to take responsibility for the professional cybersecurity training in the country.

R3.16 Task the dedicated body to work with relevant role players a framework for certification and professional accreditation in cybersecurity fields within the public and critical infrastructure sectors in Cape Verde.

R3.17 Task the dedicated body to work with relevant role players to establish basic training requirements for cybersecurity professionals within the public and critical infrastructure sectors.

R3.18 Task the dedicated body to work collaboratively with stakeholders from higher education, and the private and public sectors to identify training needs and to develop an industry-based learning programme that will enable students to gain practical experience in cybersecurity practice and use of technology.

R3.19 Use government incentives to encourage investment in creating training centres that would offer seminars and cybersecurity professional training. Incentivise companies to send their employees to cybersecurity training.

R3.20 Task the designated body to work collaboratively with the public and private sectors as well as academia and civil society to establish a national

body of (certified) cybersecurity professionals focused on knowledge transfer and advancing the cybersecurity profession within the country.

R3.21 Task the dedicated body to create some measurement system, with relevant metrics, to determine professional training take-up, including a feedback mechanism. Use feedback and lessons learnt to revise course content and design to meet current and emerging requirements.

R3.22 Task the dedicated body to determine the demand for cybersecurity trained professionals, as well as the demand for such professionals. Use these statistics in relevant planning.

R3.23 Task the dedicated body to Market Cybersecurity as a professional career path through different media.

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: Formative to Established

Cape Verde updated its legislation in 2017 as part of the Budapest convention ratification process. The new comprehensive ICT legislative and regulatory framework addresses cybersecurity, and also the protection of the rights of individuals and organisations that evolve in the digital environment. Specific legislation includes privacy, data protection, electronic transactions, substantive and procedural criminal law.

In 2007, Cape Verde repealed the electronic commerce law 49/2003 which was based on the UCNITRAL laws on electronic commerce[25] and adopted the Decree-Law No. 33/2007[26]. This new law, along with the Decree 18/2007 regulate the procedures

[25] https://uCNItral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status
[26] https://unctad.org/en/PublicationsLibrary/dtlstict2015d2_en.pdf

underpinning electronic commerce in Cape Verde. These laws also govern the use of the electronic signature. Decree No. 42/2006[27], and Decree N0. 4/2007 define the application, the requirements and the use of electronic invoices. In 2009, the Decree-Law No. 44/2009 was adopted for the establishment of a Public Key Infrastructure (KPI) which facilitates the secure electronic transfer of information.

Computer security offences are covered under the Cape Verde penal code of 2003[28]. For instance, illegal computer processing, which criminalises the processing of data without authorisation, is covered by article 187. Article 212 criminalises the use of a computer to commit fraud. Such fraud includes inputting false or incorrect data, outputting inaccurate data, or programmes that aim to commit fraud.

According to CMM participants, domestic law recognises fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. Articles 41 and 42 of the constitution also guarantee the confidentiality of a person's communications, unless otherwise authorised by a court order. It is important to note that the government of Cape Verde established the Comissão Nacional de Protecção de Dados[29] as the national data protection authority. Law No. 41/VIII/2013 covers the protection of personal data[30].

The Commission has multiple responsibilities which include but not limited to (i) to authorise or register the processing of personal data; (ii) to allow the use of personal data for purposes other than collection; (iii) to authorise, in cases provided by law, the interconnection of automated processing of personal data; (iv) to authorise the transfer of personal data; (v) to set the retention period for personal data, according to the purpose of the request; (vi) to guarantee the right of access to information, as well as the right of rectification; (vii) to receive complaints, grievances or petitions from citizens; (viii) to waive the execution of security measures provided by law, and give directives to certain sectors of activity; (ix) to promote the dissemination and clarification of data protection rights; and, (x) to promote and appreciate codes of conduct.

General consumer protection legislation protecting consumers has been adopted since 1998 with Law No 88/V/98[31]. However, it did not contain provisions that address e-commerce specifically. So, in 2007, law No 46 was enacted to cover all advertising practices, including online advertising. Article 35 of this law requires service providers to make information available to consumers about the product or service being advertised. It also requires senders of unsolicited advertisements to provide the receiver with a means to request removal from the mailing list. Even though these

[27] https://unctad.org/en/PublicationsLibrary/dtlstict2015d2_en.pdf
[28] https://unctad.org/en/PublicationsLibrary/dtlstict2015d2_en.pdf
[29] http://www.cnpd.cv/
[30] https://kiosk.incv.cv/1.1.48.1743/
[31] http:// adeco.cv.free.fr/Law_consumidor.htm

provisions exist, most participants stated that they are not aware of any consumer protection law that covers online matters in Cape Verde. They do not know whom to contact in case of a dispute.

While Cape Verde has not adopted specific legislation on Child Online Protection, article 9 of Law No. 8/IX/2017 on cybercrime firmly condemns the production, the diffusion, and the broadcasting of child pornography. However, participants believe that the law does not go far enough to protect the children and reprehend behaviours such as child online harassment.

Participants of the CMM review also noted that, even though there is general intellectual property legislation in Cape Verde, digital intellectual property is not covered.

Substantive and procedural cybercrime legal provisions are addressed by Law No. 8/IX/2017 on cybercrime and the general criminal law. Cape Verde Parliament adopted Law No. 8/IX/2017 in November 2006, and it entered in effect in March 2017, as part of the Budapest Convention ratification**.** The law covers provisions on the collection of digital evidence, on cybercrime and international cooperation. For instance, article 13 covers the scope of procedural provisions; article 14 covers data preservation, the processes to request data preservation, the responsibility of service providers while preserving data; and the role of the judicial authority during a renewal of data preservation. The law also covers the situations under which the competent legal authority can order an organisation or a person to provide access to a specific computer system. Computer search, seizure of electronic documents, and seizure of email communication records are also governed by chapter 3 of Law No. 8/IX/2017 on cybercrime.

It is important to note that, to date, the legislative framework for ICT Security which is critical to make sure all the CNI stakeholders follow minimum requirements as far as cybersecurity is concerned, is still to be developed. For instance, during the CMM review, participants stressed the need for a comprehensive law addressing the protection of critical national infrastructure and the roles and responsibilities of the CNI operators.

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: Formative

In Cape Verde, all entities of the criminal justice system seem to have been created. According to participants to the CMM consultations, a specialised unit within the judiciary police was established in 2017 and tasked with investigating cybercrimes. This brigade is composed of five members, including three inspectors. Participants also mentioned that the members of the unit had received extensive training on cybercrimes and ICT. However, they believe that due to limited resources, the brigade is not as effective as it should be. As an example, the unit does not have a functional forensic lab, it is not equipped for cybersecurity surveillance, and only has a handful of specialised cybercrime investigation officers.

It is also important to note that no mandatory cybercrime training has been developed or instituted inside the national police. Participants confirmed that law enforcement officers had received ad-hoc trainings, from international partners such as Council of Europe and Interpol, on general cybercrime and digital evidence. However, no participant was able to confirm the number of law enforcement agents who receive such training.

As to the court system, it was reported that some training sessions had been held for some judges and prosecutors, but it is unclear how much of the content was tailored to the local legislation and how many professionals attended. During the CMM review, participants mentioned that the public ministry has tried to bring all the magistrates to the specialised training sessions that it offers, but so far, this initiative has been unsuccessful due to scheduling conflicts.

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

Stage: Established

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.

As part of the ratification of the Budapest convention, Cape Verde has established an international and mostly multilateral formal cooperation mechanism to combat cybercrime by facilitating its detection, investigation, and prosecution. Examples of cooperation include preservation and disclosure of computer data, access to computer data, and seizure and disclosure of data stored in a computer system located in Cape Verde. The grounds for refusal of international cybercrime requests are covered by article 25 of Law No. 8/IX/2107. Participants of the CMM review reported that there is a robust collaboration mechanism on cybercrime with Interpol, the Council of Europe, Portugal, and Ecowas countries.

At the national level, Law No. 8/IX/2017 on cybercrime states that the competent authority, on the requisition of the prosecutor or order of the investigating judge, is authorised to collect, record, or maintain by any technical means, data associated with a specific computer system or communication. It can also compel a service provider, within the scope of its existing technological capabilities, to assist in collecting or recording data related to communication within the territory.

In practice, regional and national interagency cooperation is an issue. Most cooperation with neighbouring countries is done informally. The process for interagency collaboration is believed to be time-consuming, especially the interaction between law enforcement and ISP as no communication channel for the ISP to provide the requested information has been defined as yet. On the other hand, there is optimism as participants believe that the country is in the process of digitising procedures, which will make it more efficient. Participants also mentioned that it is common practice to start such operations informally, but eventually, all the formal steps will have to be followed, and the required paperwork submitted.

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 Cape Verde. 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 on ICT security. Ensure such legal framework also meets Cape Verde's international commitments (e.g., treaties, conventions).

R4.3 Ensure that a specific national child protection online law is successfully enacted and implemented per international and regional standards and best practices. Also, ensure that legal mechanisms are in place that enable its enforcement, including the establishment of a coordination and monitoring agency.

R4.4 Ensure the development and implementation of specific provisions and procedures in the current or new consumer protection legal framework meet international standards and best practices in the application of technology to consumer protection.

R4.5 Ensure that a specific intellectual property protection online law or provision is enacted and implemented per the international standards and best practices.

R4.6 Review and implement specific legal provision on e-commerce concerning cybercrime incidents, such as online fraud, spam, and phishing sites.

R4.7 Consider ratifying and implementing the Malabo convention.

CRIMINAL JUSTICE SYSTEM

R4.8 Invest in advanced investigative capabilities to allow the investigation of complex cybercrime cases, supported by regular testing and training of law enforcement officers and investigators.

R4.9 Allocate resources dedicated to making the cybercrime unit fully operational to support investigations nationwide. Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources.

R4.10 Develop and institutionalise specialised training programmes for law enforcement officers, including police, prosecutors and judges on cybercrime, electronic evidence and personal data protection matters. Consider establishing standards for training of law enforcement officers working on cybercrime.

R4.11 Build a cadre of prosecutors and judges, specialised on cybercrime and electronic evidence, to investigate, prosecute and process cybercrime-related cases.

R4.12 Establish formal mechanisms, protocols and best practices to enable information sharing and cooperation between prosecutors, judges and the cybercrime unit of the judiciary police in order to ensure efficient and effective prosecution.

R4.13 Collect and analyse statistics and trends regularly on cybercrime investigations, prosecutions and convictions, to inform decision making.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.14 Facilitate and encourage informal cooperation mechanisms within the law enforcement and criminal justice system, and between law enforcement and third parties such as ISPs.

R4.15 Allocate resources to support information sharing between the public and private sectors at the national level and enhance supporting 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

At the time of the CMM review, no specific cybersecurity-related standards nor framework were adopted for use within government entities in Cape Verde. Government entities mostly relied on the technical controls implemented by NOSi, the body responsible for operating the government ICT infrastructure. NOSi relies on various sources for security controls but has not fully implemented any specific cybersecurity standards and/or framework.

Within the private sector, no cybersecurity standards nor good practices have been promoted and the adoption of international standards is still very low. Banks and Financial institutions are further advanced in applying cybersecurity standards thanks to contractual obligations such as PCI DSS and the Swift cybersecurity framework. A few participants from the financial sector also indicated that their institutions have

selected and implemented ISO27001 for managing information security with some personnel being certified.

Participants also agreed that no standards or good practices had been identified for use in guiding the procurement process for the public or private sectors. Some participants did report initiatives toward formalising such practices, especially within the financial sector.

Very little was said about software development during the focus groups, but participants agreed that no standards nor good practices for software development have been identified for use relating to integrity and resilience in the public or the private sectors. Institutions and corporations mostly rely on their internal general project management and/or software development process but not necessarily on specific standards.

Furthermore, no evidence of synergy between government and the private sector to harmonise approaches towards implementation of cybersecurity standards was reported to the review team.

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: Formative

At the time of the review, Cape Verde relied on the WACS as sole submarine cable for accessing the Internet. The EllaLink[32] project, which is a submarine cable linking Brazil and Portugal via Cape Verde, would address the redundancy for Internet connectivity for the country and will also bring an additional 400 Gbps capacity. To connect the islands, a redundant fibre loop has been deployed and is fully operational. Telecommunication infrastructure is owned and managed by a government-owned company. Two companies operate in the retail market.

The majority of the people in Cape Verde accesses the Internet through their mobile phone.

[32] https://www.globenewswire.com/news-release/2018/12/13/1666520/0/en/Cape-Verde-Telecom-and-EllaLink-sign-agreement-for-connectivity-to-Cape-Verde-on-the-EllaLink-Submarine-Cable-System.html

There was a consensus that Internet access was of good quality in Cape Verde. Participants indicated that the availability of the service was good, and the cost was deemed affordable, especially for mobile.

To improve the connectivity and set foundations for it key objective of creating a regional digital hub in Cape Verde, the government has also been promoting Public-Private Partnerships and Direct Private Sector Investments in order to stabilise, explore and preserve the following: (i) the launch of the network "Amílcar Cabral" consisting of fibre optic cables for sub-regional capitals Nouakchott, Dakar, Banjul, Bissau, Conakry, Freetown and Monrovia (ECOWAS); (ii) the connection to the fibre optic cable PEACE, through South Africa and Mozambique (CPLP); (iii) the launch of fibre optic cable DILCE between Cape Verde and the United States (Boston); (iv) the renewal and implementation of "sub-loops" on the network of fibre-optic inter-island; (v) the building the Data Center of Mindelo (DC3); and, (vi) the Data Center Expansion Beach (DC2).

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 development, deployment, maintenance and updates are not standard in Cape Verde. 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 even though changes in the new software supply chain management is being efficient in reducing such practice.

Participants also advised that the top priority for companies when acquiring a software product would be the price and that the basic functionality, software quality and security requirements would be secondary concerns.

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 varies across sectors and organisations in Cape Verde. 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 sectors.

It also appears that ISPs 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 own devices.

As for basic Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS), they are rarely deployed outside of the leading companies.

In general, the level of understanding and deployment of security controls appears to be low in Cape Verde as many participants reported that they mainly rely on international partners and service providers to define and implement such controls.

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: Formative

Cryptographic controls for protecting data have been recognised by the public sector in Cape Verde. To support the uptake of e-government services, a National Public Key Infrastructure (PKI) has been established, and cryptographic based state-of-the-art controls have been implemented within the government infrastructure and platforms.

Within the financial sector, data are routinely encrypted in transit, but the capacity to deploy cryptographic controls is still lacking across sectors.

State-of-the-art tools such as TLS and SSL might be deployed in an ad-hoc manner by web service providers, but routine use of those controls is yet to come.

D 5.6 CYBERSECURITY MARKETPLACE

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

Stage: Start-up

No domestic market for cybersecurity technologies and cybercrime insurance products has yet been developed in Cape Verde. While international providers offer a range of cybersecurity products for local 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. 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 Cape Verde. 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 programme to identify, adapt and adopt international information risk management standards and frameworks applicable to the public sector and government agencies.

R5.2 Promote the adoption of international cybersecurity standards and good practices to support procurement processes within the public and the private sectors.

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

R5.4 Promote adoption and implementation of international IT and cybersecurity standards such as ISO27001, NIST CSF across private sector companies.

INTERNET INFRASTRUCTURE RESILIENCE

R5.5 Enhance coordination regarding the resilience of Internet infrastructure across the public and private sectors and expand the national programme 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 is applicable across all government entities and encourage the private sector to do likewise.

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

TECHNICAL SECURITY CONTROLS

R5.10 Promote the development of repositories of up-to-date technical security controls in both the public and private sectors. Those controls could be inspired by international repositories such as the "CIS Critical Security Controls" or ISO27001.

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

R5.12 Promote (private and public-sector) professional 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 the private sector and critical infrastructure for the protection of data at rest and in transit, according to international standards and guidelines.

R5.15 Encourage web-service providers to deploy state-of-the-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 for secure communication services, such as encrypted and electronically signed emails.

CYBERSECURITY MARKETPLACE

R5.17 Incentivise private sector and academia to invest in cybersecurity technological research and development. Encourage region-wide level initiative through academia.

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

R5.19 Promote sharing of information and best practices among organisations, to encourage the development of a 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 acknowledgement report.

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 with the notable exception that no participation from the telecommunication sector was recorded. Fortunately, a representative of the review team had met separately with all telecommunication operators and ISPs at an exploratory and pre-assessment visit and gathered enough information to serve the purpose of this review.

This was the 21st country review using the CMM framework in Africa.

THE WORLD BANK

1818 H Street, NW Washington, DC 20433 USA

Tel : (202) 473-1000

Web: www.worldbank.org