Cybersecurity Capacity Review of the Republic of Madagascar

Global Cyber Security Capacity Centre

University of Oxford

22/11/2016

Lead researchers: Ms Eva Ignatuschtschenko and Mr Taylor Roberts

Reviewed by: Professor Ivan Arreguín-Toft, Professor Paul Cornish, Professor Sadie Creese, Professor William Dutton, Professor Michael Goldsmith, Ms Lara Pace, Professor Basie Von Solms

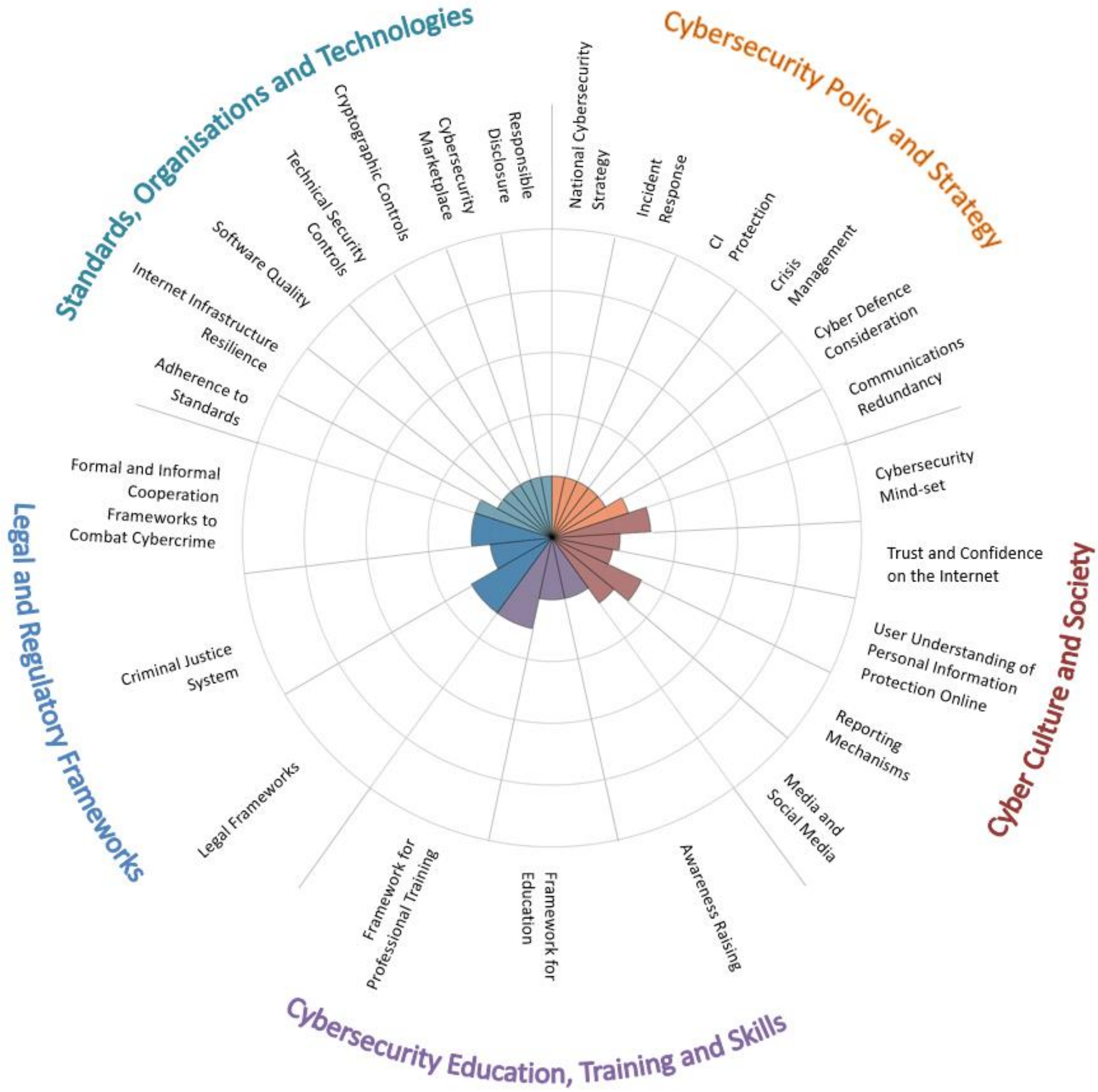
Approved by: Professor Michael Goldsmith

Contents

List of Abbreviations

ARTEC	Agency for Regulation of Technology and Telecommunication *(Autorité de Régulation des Technologies de Communication)*
CI	Critical Infrastructure
CIRT	Computer Incident Response Team
CMM	Cybersecurity Capacity Maturity Model
CSIRT	Computer Security Incident Response Team
EASSy	Eastern Africa Submarine Cable System
GCSCC	Global Cyber Security Capacity Centre
IGO	Intergovernmental Organisation
ICT	Information and Communication Technologies
InATA	Institute of Arts and Advanced Technologies (*Institut des Arts et des Technologies Avancées*)
INTERPOL	International Criminal Police Organization
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
LION	Lower Indian Ocean Network
MDN	Ministry of National Defence *(Ministère de la Défense Nationale)*
NGO	Non-governmental Organisation
NIC-MG	Network Information Center Madagascar
SME	Small and medium-sized enterprise

Executive Summary



In collaboration with the International Telecommunication Union (ITU), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') was invited to undertake a review of the maturity of cybersecurity capacity in the Republic of Madagascar. The review was hosted by the Agency for Regulation of Technology and Telecommunication (*Autorité de Régulation des Technologies de Communication*), ARTEC. The objective of the review was to enable the Republic of Madagascar to gain an understanding of its cybersecurity capacity in order to develop an investment strategy for the development of Madagascar's cybersecurity capacity.

Between 24th and 26th August 2016, stakeholders from the following sectors participated in roundtable consultations: public sector entities, academia, civil society, legislators and policy makers, information technology officers from government and the private sector, Internet Service Providers and the banking sector. The consultations were centred upon the Centre's

Cybersecurity Capacity Maturity Model (CMM), which defines five areas of cybersecurity capacity:

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

Cybersecurity Policy and Strategy

The *Cybersecurity Policy and Strategy* dimension of cybersecurity capacity for the Republic of Madagascar was identified to range from *start-up* to *formative* stages of maturity. Even though cybersecurity has emerged as an emerging priority across government and private sector entities, the development of a national cybersecurity strategy has not yet commenced. Sectoral strategies exist, for instance in the finance sector, but these are limited to the respective industry and responsible government agency.

Similarly, incident response is provided *ad hoc* by telecommunications operators rather than a national computer security incident response team (CSIRT), which poses a challenge to effective and coordinated incident response and management. No regulation is in place that requires incidents to be reported and Madagascar as yet has no mandated authority or protocol to handle such a process.

Work on a central list of critical infrastructure (CI) assets has not yet commenced. Communication between the government and CI operators is *ad hoc* and therefore coordination is limited. In cases where a coordinated response would be required, there is neither a cybersecurity operational plan in place, nor is a government agency mandated to manage and mitigate cybersecurity incidents. Similarly, risk management exercises or cyber security drills are not yet conducted at a national level.

In the case of crisis management, national planning and evaluation of crisis management protocols and procedures is taking place for natural catastrophes. However, these plans and evaluations do not yet incorporate cybersecurity elements.

The Republic of Madagascar does not have a specific cyber Defence policy or strategy. There is no strategic coordination structure for cyber Defence and operational capacity has not yet been developed, indicating that cyber Defence is not yet a priority in the national cybersecurity posture.

Communication redundancy for system fallout has been established at the organisational level in some sectors, but efforts are not yet nationally coordinated.

Overall, national *Cybersecurity Policy and Strategy* capacity in Madagascar is mostly at the initial stage of development, even though there are efforts to enhance capacity at the organisational and sectoral level. In order to elevate capacity within this dimension fully to the formative stage, our recommendations include the development of a national cybersecurity strategy, continuous work towards establishing a CSIRT and the consideration of cybersecurity in critical infrastructure protection, national defence and crisis management.

Cyber Culture and Society

National capacity in the *Cyber Culture and Society* dimension was judged to range between *start-up* and *formative* stages. Participants highlighted the private sector as being the furthest advanced with regard to cybersecurity awareness and understanding, although small and medium-sized enterprises do not yet consider cybersecurity as a priority. General cybersecurity awareness on the part of Internet users and government agencies is minimal.

Some e-government services in Madagascar have been developed, such as an online tax payment system, but uptake is low and there is currently no coordinated effort to promote and secure trust in these services. No e-commerce services have been established. Initiatives to promote trust in the use of online services are generally lacking and, consequently, the knowledge of users regarding safe online practices is limited.

Participants agreed that users mostly ‘blindly’ trust that personal information online are protected. Despite the recently adopted data protection legislation, doubts were raised regarding the handling of data that are shared online, while the average user lacks awareness and understanding of personal information protection online.

No central dedicated mechanism was identified that enables citizens to report computer-related or online incidents and crimes has been established in Madagascar. Through an initiative led by UNICEF, crimes relating to online child abuse can be reported online or via phone, but there is no similar channel for other types of cybercrime.

Finally, media and social media are not yet taking an active role in reporting cybersecurity threats and incidents or raising awareness of cybersecurity across broader society. In particular, the media cannot yet effectively communicate measures users can take to protect themselves online.

Within this dimension, Madagascar has almost achieved the formative stage of capacity. Measures that promote the safe use of online services, raise user awareness of risks and threats in the online environment, and enable citizens to report online incidents, would facilitate the increase of capacity across the *Cyber Culture and Society* factors.

Cybersecurity Education, Training and Skills

Consultations indicated that the *Cybersecurity Education, Training and Skills* capacity in Madagascar ranged from the *start-up* to *formative* stage. As ICT infrastructure and services are only starting to spread across the country, cybersecurity awareness-raising has not yet gathered momentum. Some *ad hoc* awareness-raising initiatives have been created, but these lack coordination.

At the university level, limited educational offerings are available in computer science, but there are no specific cybersecurity modules or courses. Educational programmes on information and communications technology (ICT) including emphasis on related security challenges have not yet been developed at all levels of education. Cooperation between educational institutions and the private sector is lacking.

Some *ad hoc* training on IT security is offered in Madagascar, but cybersecurity training needs in the public and private sector have not yet been documented and coordination between training providers, as well as between academia and the private sector, is minimal. Transferring knowledge between employees and linking awareness-raising efforts with training programmes were noted as important steps towards the efficient enhancement of capacity within this dimension. We further recommend the development of a national cybersecurity awareness programme and the creation of specialised university degree programmes in information security, cryptography and network security with cybersecurity modules.

Legal and Regulatory Frameworks

Legal and Regulatory capacities were judged to range between the *start-up* and the *formative* stages of maturity. Components of a broad cybersecurity legal and regulatory framework were adopted in Madagascar in 2014 and 2015, but implementation of the laws is still insufficient to reach the established stage. Moreover, gaps and inconsistencies have been identified in existing laws, which require revision and expansion of the legal framework. Some legal aspects, such as consumer protection online, are not yet being discussed amongst the legal community.

Regarding operational capabilities, law enforcement has some capacity to investigate computer-related crimes, but specialised and institutionalised training is not available for law enforcement officers, thus limiting investigative capabilities. Prosecutors and judges are not trained adequately and do not have the capacity to prosecute and preside over computer-related crimes. Human, financial and technical resources across the criminal justice sector are considered to be insufficient by the review participants.

Domestic and international cooperation to combat cybercrime is largely informal in nature, for example through the International Criminal Police Organization (INTERPOL). Formal mechanisms that complement these informal relationships have not yet been established.

In order to enhance *Legal and Regulatory* cybersecurity capacities in Madagascar, we inter alia recommend the revision or adaptation of the legal framework to address gaps, the institutionalisation of specialised training for all parts of the criminal justice system, as well as the establishment of mutual legal assistance and extradition instruments to combat cybercrime.

Standards, Organisations, and Technologies

Madagascar's capacity in *Standards, Organisations and Technologies* was assessed to range from the *start-up* to the *formative* stages. No coordinated effort to adopt and implement cybersecurity standards could be ascertained. The adoption of standards varies from organisation to organisation, in accordance with individual needs and the requirements of parent organisations, but there is no coordination across sectors. Procurement and software development standards are partly applied but, overall, the strategic focus is primarily on function and price.

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

When reviewing the security measures deployed across different industrial sectors in the country, the level of capacity varies significantly depending on the priority placed on cybersecurity. Software quality is not monitored and there is no catalogue of secure software platforms and applications. ISPs do not offer anti-malware software as part of their services and users only have a limited understanding of the available technical security controls. Similarly, cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and in transit have been identified as a concern, but are not yet deployed consistently within the government, the private sector and the general public.

No domestic market for cybersecurity technologies and cybercrime insurance products has yet been developed. While international providers offer a range of cybersecurity products for domestic use, there are no domestic commercial cybersecurity products or cybercrime insurance offerings on the Malagasy market.

Overall, capacities within this dimension are mostly at the initial level of development. In order to enhance cybersecurity capacities relating to *Standards, Organisations and Technologies*, we recommend to develop policies and programmes that encourage the adoption of international IT standards, promote secure hardware and software deployment and maintenance, enhance internet infrastructure resilience and expand the use of technical security controls and cryptographic controls. We further encourage the consideration of developing a cybersecurity marketplace and a national responsible disclosure framework.

Additional Reflections

This was the thirteenth country review supported directly by the Global Cyber Security Capacity Centre at Oxford, and the second conducted in collaboration with the International Telecommunication Union (ITU). This review has assisted the Government of the Republic of Madagascar to gain insights into the breadth and depth of the country's cybersecurity capacity. Madagascar has commenced the process of developing different aspects of cybersecurity capacity across all dimensions, including through developing a broad legal framework and the gradual expansion of cybersecurity training offerings. These efforts will set the foundations for more advanced capacity in the future. The review suggests a number of specific steps by which Madagascar's cybersecurity capacity might achieve greater levels of maturity and might contribute to the development of a National Cybersecurity Strategy and a national CSIRT/CIRT.

The Global Cyber Security Capacity Centre

Introduction

In collaboration with the International Telecommunication Union (ITU), the Global Cyber Security Capacity Centre (GCSCC) was invited to facilitate a review of cybersecurity capacity maturity in the Republic of Madagascar, hosted by the national host team from the telecommunications agency *Autorité de Régulation des Technologies de Communication* (ARTEC). The objective of this exercise was to enable the national stakeholders to prioritise areas of capacity in which the country might seek to make strategic-level investment, in order to improve Madagascar's national cybersecurity posture.

From 24th to 26th August 2016, stakeholders from the following sectors participated in a four-day consultation to review the cybersecurity capacity of the Republic of Madagascar:

- Public Sector Entities:
    - Agency for Regulation of Technology and Telecommunication (*Autorité de Régulation des Technologies de Communication, ARTEC*);
    - Ministry of Post, Telecommunications and New Technologies (*Ministère des Postes, des Télécommunications et du Développement Numérique, MPTDN*);
    - Ministry of National Defence (*Ministère de la Défense Nationale, MDN*);
    - Ministry of Finance and Budget (*Ministère des Finances et du Budget, MFB*);
    - Ministry of Justice (*Ministère de la Justice*);
    - Ministry of Public Security (*Ministère de la Sécurité Publique*);
    - Ministry of Population, Women and Children (*Ministère de la Population, de la Condition Féminine et de l'Enfance*);
    - Financial Intelligence Service (*Service de Renseignements Financiers, SAMIFIN*).
- Legislators/Policy Makers
- Criminal Justice and Law Enforcement
- Armed Forces
- Senators
- Academia
- Civil Society
- Private Sector
- Telecommunications Companies
- Finance Sector

Consultations were framed by the GCSCC's Cybersecurity Capacity Maturity Model (CMM) which is composed of five dimensions of cybersecurity capacity:

1. Cybersecurity Policy and Strategy;
2. Cyber Culture and Society;
3. Cybersecurity Education, Training and Skills;
4. Legal and Regulatory Frameworks;
5. Standards, Organisations, and Technologies.

Each dimension consists of a set of factors, offering a more detailed explanation of cybersecurity capacity. Table I below shows the five dimensions with their respective factors:

Table I: Description of Factors within Each Dimension

Dimension	Factors
Dimension 1 Cybersecurity Policy and Strategy	F 1.1: National Cybersecurity Strategy
	F 1.2: Incident Response
	F 1.3: Critical Infrastructure (CI) Protection
	F 1.4: Crisis Management
	F 1.5: Cyber Defence Consideration
	F 1.6: Communications Redundancy
Dimension 2 Cyber Culture and Society	F 2.1: Cybersecurity Mind-set
	F 2.2: Trust and Confidence on the Internet
	F 2.3: User Understanding of Personal Information Protection Online
	F 2.4: Reporting Mechanisms
	F 2.5: Media and Social Media
Dimension 3 Cybersecurity Education, Training and Skills	F 3.1: Awareness Raising
	F 3.2: Framework for Education
	F 3.3: Framework for Professional Training
Dimension 4 Legal and Regulatory Frameworks	F 4.1: Legal Frameworks
	F 4.2: Criminal Justice System
	F 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 Standards, Organisations, and Technologies	F 5.1: Adherence to Standards
	F 5.2: Internet Infrastructure Resilience
	F 5.3: Software Quality
	F 5.4: Technical Security Controls
	F 5.5: Cryptographic Controls
	F 5.6: Cybersecurity Marketplace
	F 5.7: Responsible Disclosure

Each factor comprises a number of maturity indicators with which a country's cybersecurity capacity can be gauged. These maturity indicators are further organised into five ascending stages, from 'start-up' to 'dynamic'. The five stages are 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 at this stage.
- **Formative:** Some features of the aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply "new". However, evidence of this activity can be clearly demonstrated.

- **Established:** The elements of the aspect are in place, and working. There is not, however, well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the “relative” investment in the various elements of the aspect. But the aspect is functional and defined.
- **Strategic:** Choices have been made about which parts of the aspect are important, and which are less important for the particular organisation or nation. The strategic stage reflects the fact that these choices have been made, conditional upon the nation or organization's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technology of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this stage.

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

Cybersecurity Context in Madagascar

The development and expansion of Internet infrastructure in Madagascar is still at an early stage and Internet penetration in the country is still relatively low. As few as 11% of the population are connected to the Internet. However, Internet usage is rapidly increasing as infrastructure becomes more reliable, for two reasons. First, international submarine fibre optic cables, Lower Indian Ocean Network (LION) and Eastern Africa Submarine Cable System (EASSy), were landed in Madagascar in 2009 and 2010, thereby enabling independence from satellites for international connections and making internet access more affordable.[1] Second, Madagascar launched a new Internet exchange point, the Madagascar Global Internet eXchange (MGIX) in 2016, which enhances Internet speed and decreases international bandwidth costs.[2] Moreover, a national optic fibre backbone to connect major cities across the country is being put in place.

Alongside improved Internet performance, Madagascar has also seen the emergence of various forms of cybercrime, varying in their severity. According to review participants, common forms of cybercrime in Madagascar include computer-related fraud (in particular on social media platforms or related to mobile banking), cyber harassment, hacking, Distributed Denial of Service attacks (DDoS) and website defacement.

As a result of these developments, Madagascar has started to prioritise the security of the Internet, most prominently by the adoption in 2014 and 2015 of a number of laws relating to cybersecurity (see Dimension 4 below). At the time of the review, leading stakeholders in promoting the advancement of national cybersecurity capacity include the Telecommunications Regulatory Authority (*Autorité de Régulation des Technologies de Communication*), the Ministry of Post, Telecommunications and New Technologies (*Ministère des Postes, des Télécommunications et du Développement Numérique*), the Ministry of Justice (Ministère de la Justice), the Ministry of Public Security (*Ministère de la Sécurité Publique*), the Network Information Center Madagascar (NIC-MG) and the Internet Society chapter of Madagascar.

Review of Cybersecurity Capacity Maturity: General Observations

Graphic I presents the maturity estimates in each of the five CMM dimensions. 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.

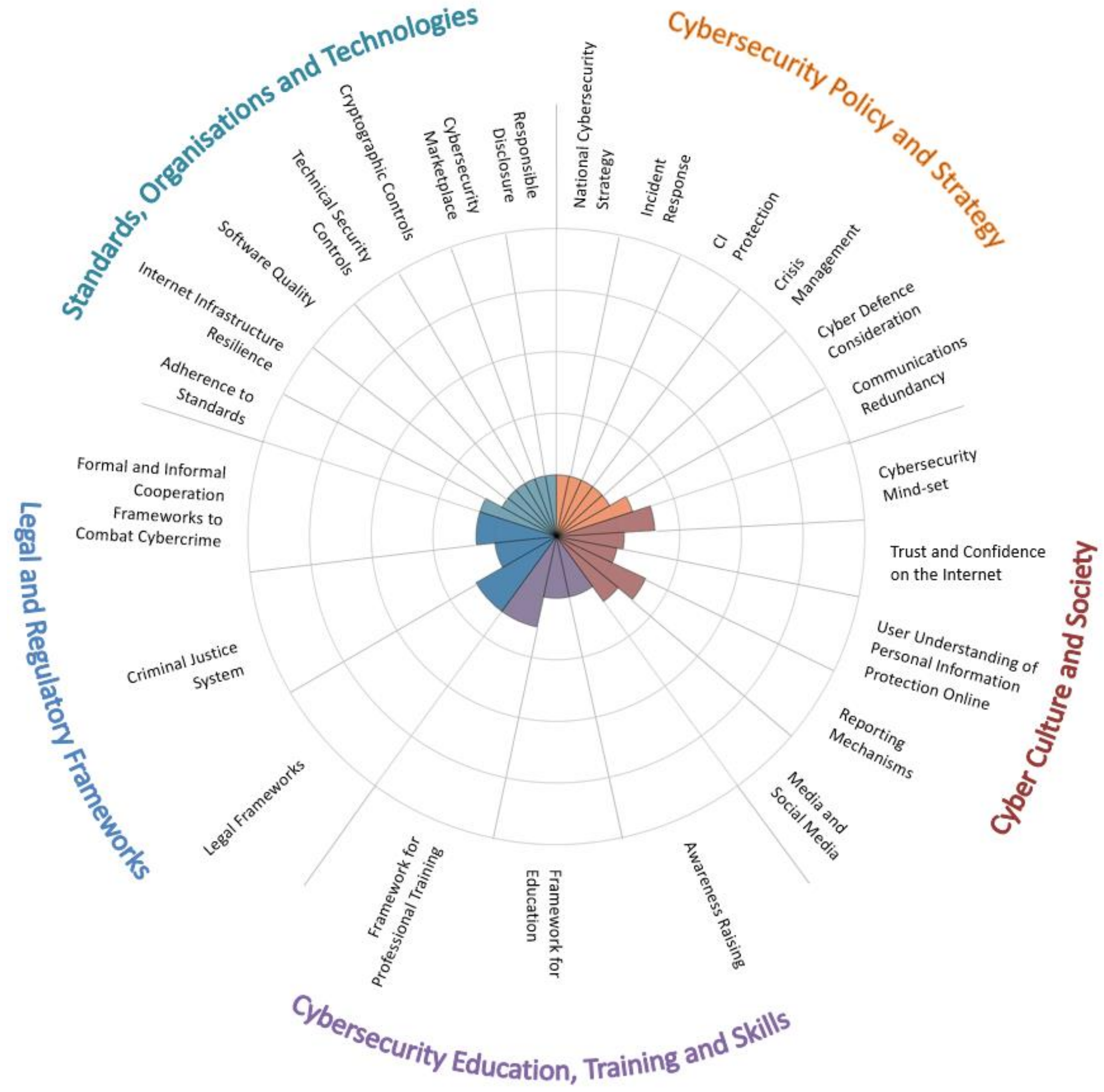
Graphic I shows that Madagascar has achieved start-up in all aspects of the CMM and is evolving towards achieving a formative stage in almost half of the model. The CMM methodology requires all the indicators for a certain stage to have been met before that stage of maturity can be assigned. In other words, maturity in cybersecurity is assessed and attributed only according to the highest completed stage.

[1] See https://www.budde.com.au/Research/Madagascar-Telecoms-Mobile-Broadband-and-Digital-Media-Statistics-and-Analyses.

[2] See http://au.int/ar/sites/default/files/PR%20088-%20IXP%20Launch%20in%20Madagascar.pdf.

Appendix I presents a summary of the results for each factor, including a brief description of those results. Links to key policy and strategy documents, laws and other additional information are also provided. Appendix I also presents a total of seventy-two recommendations regarding the enhancement of the existing capacity for each factor.

Graphic I: Review Results



Dimension 1: Cybersecurity Policy and Strategy

Dimension 1 gauges Madagascar's capacity to develop and deliver cybersecurity policy and strategy and to enhance its cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection. Cybersecurity policy and strategy also includes consideration of 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.

F 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 cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

There is currently no official national cybersecurity strategy document in Madagascar, which would establish coordination of the various existing initiatives and activities, as set out in the factors below. While laws and regulations were adopted in recent years that address cybersecurity concerns in broad scope (see Dimension 4 below), these developments were not accompanied by the development of an overarching strategic framework to coordinate and prioritise measures to enhance Madagascar's cybersecurity capacity.

Sectoral strategies exist and have been developed in cooperation with international partners, such as the World Bank, and a national ICT policy was developed in conjunction with the United Nations Development Programme (UNDP), but this policy was never implemented.

In order to ensure that national efforts to advance cybersecurity capacity across all dimensions and parts of the nation are harmonised and coordinated effectively, the development of national cybersecurity policy and strategy is considered to be international best practice. This process should include all relevant stakeholders and should be accompanied by a national programme to implement the policy. In the course of the review several key institutions were mentioned which should be considered for the development and implementation of a national cybersecurity strategy, including: the Telecommunications Regulatory Authority (*Autorité de Régulation des Technologies de Communication*), the Ministry of Post, Telecommunications and New Technologies (*Ministère des Postes, des Télécommunications et du Développement Numérique*), the Ministry of Justice (*Ministère de la Justice*), the Ministry of Public Security (*Ministère de la Sécurité Publique*), and the Internet Society chapter of Madagascar. The multi-stakeholder approach followed during the national Internet Governance Forum (IGF) could serve as a model to engage with stakeholders on the development of a national cybersecurity strategy. In light of the existing range of organisations that have taken initiative in the area of cybersecurity, the establishment of a central organisation with a mandate to coordinate the country's cybersecurity posture is a formative step towards enhancing Madagascar's cybersecurity capacity. Participants noted that rather than forming a new body to lead cybersecurity efforts in the country, an existing organisation should take the lead in order to make the most efficient use of available time and resources.

F 1.2: Incident Response

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

Stage: Start-up

Start-up Formative Established Strategic Dynamic

Currently, there is no national computer-related incident response organisation that would serve as the coordinating body for the reporting and management of cybersecurity incidents in Madagascar. Such organisations mostly take the form of Computer Security Incident Response Teams (CSIRT) or Computer Incident Response Teams (CIRT). Due to the lack of a central organisation, there is no single entity holding a central registry of national level incidents.

Ad hoc incident response is provided by telecommunications operators and the Network Information Center Madagascar (NIC-MG), but there is no coordination between those actors at the national level. If an incident occurs, the operator focuses on finding a solution to the problem, but preventive efforts are not common.

In the course of the cybersecurity capacity review, ITU conducted a readiness assessment to establish a national CIRT in Madagascar.

F 1.3: Critical Infrastructure (CI) Protection

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

Stage: Start-up

Start-up Formative Established Strategic Dynamic

The concept of cybersecurity in critical infrastructure has not yet taken hold in Madagascar. While procedures are in place to identify key infrastructures that need immediate priority in crisis situations, the notion of critical infrastructure protection does not yet go beyond emergencies. As a consequence, there is no central list of critical infrastructure assets.

Coordination among CI owners and between CI owners and the government with relation to cybersecurity threat and vulnerability disclosure is largely *ad hoc* and has not yet been institutionalised. Ministerial contact points for critical infrastructure owners have been established, but exchange of information on cybersecurity is limited and largely reactive, for instance to report security incidents to the government. A formal and/or regular process of interaction on cybersecurity issues between critical infrastructure owners has not yet been established.

General risk management and emergency response frameworks have been established across sectors and include actors such as Gendarmerie, Ministry of Defence, etc. Moreover, critical infrastructure operators conduct regular risk assessments and have organisational business continuity plans in place that address general risks, such as blackouts, natural catastrophes, etc. However, cybersecurity risks are not yet considered in the existing frameworks. Nevertheless, the existing processes could serve as a basis to integrate cybersecurity into business processes in a cost-efficient way.

F 1.4: Crisis Management

Crisis management planning addresses conducting specialised needs assessments, training exercises, and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations.

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

Even though not all participants were aware of national crisis management exercises, the National Bureau of Risk Management and Disaster Management *(Le Bureau National de Gestion des Risques et Catastrophes* - BNGRC), the operational arm of the National Council for Risk Management and Disaster (*Conseil National de Gestion des Risques et Catastrophes* - CNGRC),[3] conducts general exercises to prepare for natural catastrophes. In addition, some ISPs conduct similar exercises at the organisational level. To this date, none of these exercises have had cybersecurity elements, but the existing simulations and their evaluation mechanism could be adapted to cybersecurity incidents or to incorporate cybersecurity elements.

F 1.5: Cyber Defence Consideration

This factor explores whether the government has the capacity to design and implement a cyber Defence strategy and lead its implementation, including through a designated cyber Defence organisation. It also reviews the level of coordination between various public and

[3] See http://www.bngrc-mid.mg/.

private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

Cyber Defence capacity in Madagascar is at the *start-up* stage. Currently, there is no cyber Defence strategy and no overarching strategy or policy that would provide a framework for managing cyber Defence at the national level. The general national defence strategy does not yet recognise cybersecurity threats. Similarly, organisational security strategies have been established by critical infrastructure owners and ISPs, but there is no coordination across organisations and cybersecurity is not generally addressed in any case.

Overall, cyber Defence is not yet a priority in the national cybersecurity posture. As cyber defence capacity matures, it will need to be integrated into Madagascar's current defence sector.

F 1.6: Communications Redundancy

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

Stage: Start-up to Formative

Start-up | Formative | Established | Strategic | Dynamic

Communications redundancy as a broad concept has been considered in Madagascar, resulting in sectoral efforts to backup data and established redundant networks in cases of communication breakdown. Telecommunications operators have existing coordination mechanisms if an operator experiences interruption. Other critical infrastructure organisations might use radio communication channels in case of emergencies.

In order to increase capacity in this factor, better coordination of the various efforts regarding communications redundancy should be sought. Participants highlighted the need to ensure uninterrupted functionality of the systems and the zero tolerance of network breakdown for Internet service providers.

Recommendations

The following recommendations are intended to increase existing cybersecurity capacity within the scope of Dimension 1 of the CMM: *Cybersecurity Policy and Strategy*. The recommendations are provided specifically for each factor.

National Cybersecurity Strategy

Improvements in Madagascar's national cybersecurity capacity will to a considerable extent be contingent upon the development and articulation of a national cybersecurity strategy:

- **R1-1:** A formal decision by the Government of Madagascar to embark upon a National Cybersecurity Strategy. This document should set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. The strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives.
- **R1-2:** Allocate budget and assign a government agency to oversee the implementation of the National Cybersecurity Strategy, taking into account existing roles and responsibilities.
- **R1-3:** Design and disseminate coordinated cybersecurity programmes.
- **R1-4:** Strengthen and promote inter-departmental cooperation in cybersecurity.

Incident Response

Without a national CSIRT/CIRT or other central computer-related incident response body, there will be no effective way to share information and resolve incidents at the national level. Communication channels between actors remain *ad hoc* and inconsistent, impeding effective incident management. The following recommendations are to be considered:

- **R1-5:** Continue work towards the development of a national CSIRT/CIRT with clear processes and defined roles and responsibilities.
- **R1-6:** Categorise and record national-level cyber incidents in a central registry, possibly hosted by the national CSIRT/CIRT.
- **R1-7:** Draft legislation, which allocates mandates to the national CSIRT/CIRT.
- **R1-8:** Develop coordination and information/cybersecurity threat sharing mechanisms between the private and the public sector, as well as within the cybersecurity community at national, regional and international levels.
- **R1-9:** Appoint and publicize a national-level lead to ensure reporting of incidents and promote reporting.

Critical Infrastructure (CI) Protection

No central list of CI assets has been identified by the government and there is no defined cybersecurity operational plan in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber-attack on CI. Incident response by CI agencies and bodies is uncoordinated, lacking a formal cyber response plan or official mandate. Risk management exercises and drills are not conducted at a national level. The following recommendations are offered for consideration:

- **R1-10:** Develop and disseminate a list of Critical Infrastructure (CI) assets with identified risk-based priorities.
- **R1-11:** Establish a mechanism for regular vulnerability disclosure and information sharing between the public and private sector.

- **R1-12:** Establish information protection and risk management procedures and processes, supported by adequate technical security solutions, which inform the development of an incident response plan.
- **R1-13:** Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CI operators.

Crisis Management

No official planning and evaluation of cybersecurity crisis management protocols and procedures are in place. The following recommendations are offered for consideration:

- **R1-14:** Conduct a needs assessment of measures that require testing with consideration of a simple exercise scenario, potentially within the framework of the BNGRC.
- **R1-15:** Conduct compromised communication scenarios and exercises to test emergency response assets interoperability and function effectively.
- **R1-16:** Evaluate the exercises and feed the findings back into the decision-making process.

Cyber Defence Consideration

There is no defence policy or strategy for cyber Defence considerations. Operational cyber Defence capacity has not yet been developed. The review prompted the following recommendations:

- **R1-17:** Develop a cyber Defence component in the national security strategy, taking into consideration identified threats to national security in cyberspace.
- **R1-18:** Develop a communication and coordination framework for cyber Defence.
- **R1-19:** Expand coordination in response to malicious cyber-attacks on military information systems and critical infrastructure.
- **R1-20:** Conduct continuous review of the evolving threat landscape in cybersecurity to ensure that cyber Defence policies continue to meet national security objectives.

Communications Redundancy

While sectoral and organisational communications redundancy and backup systems have been implemented, these efforts are not nationally coordinated, prompting the following recommendations:

- **R1-21:** Allocate appropriate resources not solely to such activities as hardware integration, technology stress testing, personnel training and crisis simulation drills, but also to ensuring that redundancy efforts are appropriately communicated to relevant stakeholders.
- **R1-22:** Link all emergency response assets into a national emergency communication network with isolated but accessible backup systems.
- **R1-23:** Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.

Dimension 2: Cyber Culture and Society

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including users. The days in which cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programs 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 factor also entails the existence mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this factor reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

F 2.1: Cybersecurity Mind-set

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-up to Formative

Start-up › Formative › Established › Strategic › Dynamic

When reviewing the cybersecurity mind-set within Madagascar, the review looked at users and experts in three institutional settings: government, private sector, and users. Overall, our interviews found that cybersecurity has not yet become a priority across the public sector, private sector or among end-users. Some participants attributed this lack of awareness and attention to cybersecurity to infrequent national cyber-attacks, but many factors could contribute to this problem.

Among government institutions, cybersecurity is most often considered to be an IT issue to be left to the computer experts, rather than a broader organisational (and national) concern and, as such, is rarely considered by senior management. Moreover, as human and financial resources are more limited within the public sector, participants stated that the private sector has the expertise and other means to invest in cybersecurity initiatives. Some participants, on the other hand, felt that there is an increasing consciousness of cybersecurity issues among government leaders, as threats to cybersecurity are increasingly recognised as a risk to the government's authority. Moreover, recent attacks on government websites have triggered discussions towards enhancing the security of government networks and data.

While the level of understanding and general cybersecurity capacity varies widely across private sector organisations, most participants agreed that the investment into cybersecurity is generally low in the private sector, with the exception of the major ICT companies. In particular, small and medium-sized enterprises (SMEs) do not have the people or other resources to invest into cybersecurity and therefore are reliant on the cybersecurity solutions provided by computer and security firms, without any critical assessment of their quality and reliability. Nevertheless, participants indicated that the general understanding of cybersecurity risks and protective measures is further advanced in private sector organisations than in public sector institutions.

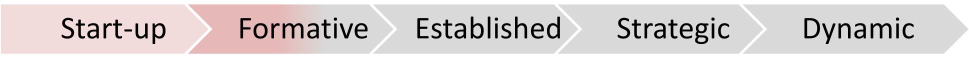
Much like the public and private sector entities, users generally have minimal levels of awareness of cybersecurity risks and secure online behaviour. Cybersecurity has not yet permeated into the daily lives of most citizens, even though they regularly engage with the Internet and related social media. Children are particularly vulnerable to cybercrime. While they are often learning how to use ICT and how to code, they can be relatively naïve about the risks of Internet use.

Even though the cybersecurity mind-set is only just beginning to develop across the various sectors of society in Madagascar, the emergence of mobile money technologies was raised as an opportunity to enhance user awareness. As access to finances is considered an essential interest in Malagasy culture, citizens are likely to become more conscious of threats relating to their financial resources. In fact, there were observations that users have been increasingly demanding of security measures to protect their mobile money transfers. This momentum could be used to enhance a cybersecurity mind-set more broadly across society.

F 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



Participants agreed that the majority of users are not worried when engaging with ICT, but mainly because of a 'blind' level of trust in technology. Usability and speed takes priority over security concerns for most users. On the other hand, participants in our interviews expressed a lack of trust in the security of online services and the protection of data.

While still at initial stages, the government has started to develop e-government initiatives, including an online tax payment system and online customs services. These developments have had a positive impact on the time required to access these services. However, multiple concerns were raised regarding the security of these government systems, for instance due to a lack of secure authentication processes, a lack of transparency and limited usability, with these new services facing regular downtimes. As a consequence, trust in e-government services was perceived to be limited.

Apart from the development of mobile money technologies, review participants were not aware of any e-commerce services offered within Madagascar. Online purchases have remained rare and mostly require the handover of payments as well as products in person. Trust in online payments and mobile money solutions has been limited precisely because of security concerns.

F 2.3: User Understanding of Personal Information Protection Online

This aspect 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

The protection of personal information online was considered of great importance to participants. The recent Law No. 2014-038 on the Protection of Personal Data (Loi n° 2014-038 sur la protection des données à caractère personnel) is an important step towards ensuring that companies implement sound data protection measures, but the law is not yet fully implemented and users are not aware of its adoption. For instance, the law requires operators to inform users of how their personal data will be used, but this measure has not yet been applied in practice. As a consequence, users are not sure about how data that they provide are used by companies. As in many other countries, participants also stated that users give away their personal details too easily and do not read terms and conditions or critically assess websites and associated risks.

In order to enhance the maturity of this factor, there is a need to fully implement the law on data protection, including monitoring of its application, and also raise awareness of users to enable them to make informed decisions when sharing their data online.

F 2.4: Reporting Mechanisms

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

Stage: Start-up to Formative

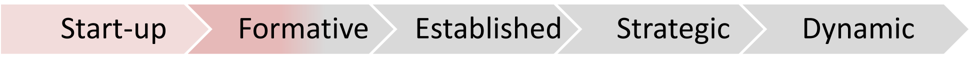
No central dedicated mechanism exists to enable citizens to report computer-related or online incidents and crimes in Madagascar. While some participants considered the general police hotline to be a first contact point to report cybercrime incidents, others did not believe that it would be the right channel, in particular for hacking incidents. Insufficient communication was raised as an obstacle to effective reporting mechanisms. The public needs to be more acutely aware of not only threats to security, but also available channels to report infringements. Moreover, coordination among the different relevant stakeholders is key to create an effective mechanism and promote trust among citizens, so that incidents are reported.

Despite the lack of a general channel to report incidents, a dedicated hotline and website was established by UNICEF in cooperation with domestic telecommunications operators for reporting of child abuse, such as online child pornography.[4] This mechanism could provide valuable insights for developing reporting channels for other types of online crime.

F 2.5: Media and Social Media

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

Stage: Start-up to Formative



Start-up Formative Established Strategic Dynamic

Mass media as well as social media have not been exploited sufficiently in threat-reporting or in raising awareness of cybersecurity in Madagascar. Media reports are mostly limited to reporting major incidents, but they could also be used productively to provide information on preventative actions that users can take to protect themselves or how to respond to cyber incidents. Likewise, cybersecurity is seldom a topic on social media platforms. Participants considered the lack of awareness among media providers to be the main reason for minimal media coverage of the topic. Enhancing the understanding of cybersecurity among media providers would facilitate a more active role of media in conveying information about cybersecurity to the public and shaping online behaviour.

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.

[4] See http://www.unicef.org/madagascar/5561_6519.html.

Cybersecurity Mind-set

To promote a stronger cybersecurity mind-set across all sectors, it is recommended to:

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

Trust and Confidence on the Internet

Trust in online services is identified as a concern that could limit initiatives in e-government and ecommerce. Users often lack knowledge regarding safe online practises and too often regard the Internet as safe, without a practical awareness of risks. E-government services are expanding, but they are not yet secure and reliable. E-commerce services are not yet available. In order to enhance the level of capacity, we suggest the following actions:

- **R2-5:** Develop campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content.
- **R2-6:** Expand e-government services with recognition of the need for the application of security measures to promote trust in e-services.
- **R2-7:** Encourage the development of e-commerce services, while emphasising the need for security.

User Understanding of Personal Information Protection Online

Stakeholders within the public and private sectors have minimal knowledge about how data are handled online, and they do not believe that adequate measures are in place to protect personal information. In order to enhance user understanding of personal information protection online, we suggest the following actions:

- **R2-8:** Establish programmes to raise user awareness of online risks and measures available to be safe online and protect privacy.
- **R2-9:** Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

Reporting Mechanisms

There is yet no centrally coordinated reporting mechanism for cybersecurity incidents in Madagascar. UNICEF is providing channels to report child online abuse, but there are no similar channels for other types of cybercrime. Therefore, the following actions are recommended:

- **R2-10:** Establish a central mechanism that allows citizens to report all types of cybercrime. Use experiences gathered through the child abuse hotlines managed by UNICEF and ISPs.
- **R2-11:** Raise awareness about existing reporting channels among the wider public.

Media and Social Media

Media rarely cover information about cybersecurity or report on issues relating to cybercrime or other incidents. Social media are not currently used to communicate and disseminate messages on cybersecurity. In order to enhance the capacity of all forms of media to disseminate information on cybersecurity, we recommend to:

- **R2-12:** Encourage media content providers to disseminate information on good cybersecurity practice, which could stimulate social media discussions on this topic.
- **R2-13:** Develop programmes to raise awareness among media and social media providers and actors on cybersecurity issues, for instance through a dedicated cybersecurity awareness month or dedicated sites on this topic.

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.

F 3.1: Awareness Raising

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

Stage: Start-up

Start-up	Formative	Established	Strategic	Dynamic

The need for cybersecurity awareness-raising programmes was acknowledged across the various stakeholder groups. However, due to the general lack of awareness of cybersecurity outside of the technical community, which is partly due to low ICT literacy, national programmes have not yet been implemented. Some participants expressed concerns regarding the security of nationwide projects involving huge volumes of data, such as a recent initiative of an international organisation that collects personal data of people living in poverty in a national database. Cybersecurity awareness, in particular in relation to the protection of personal data, needs to be prioritised for such projects. Participants also emphasised that awareness-raising programmes need to be developed alongside other capacity enhancements, such as incident response, training for cybersecurity educators, national and organisational cybersecurity policies, etc.

There are some *ad hoc* initiatives in cybersecurity awareness raising by various institutions, such as the Institute of Arts and Advanced Technologies (*Institut des Arts et des Technologies Avancées,* InATA), but these are not yet coordinated at the national level, and, therefore, a more centralised awareness-raising campaign would greatly expand fundamental understanding of cybersecurity capacity. Additionally, integrating cybersecurity awareness efforts into ICT literacy courses could provide an established vehicle for cybersecurity awareness-raising campaigns.

Among executive managers, both in public and private sectors, cybersecurity awareness is very limited, which is one reason why cybersecurity awareness raising is not yet perceived as a priority. There are no current efforts to raise the awareness of executive staff in any sector. This is an important gap, as executives are usually the final arbiters on investment into security.

F 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

Start-up Formative Established Strategic Dynamic

The development of cybersecurity educational offerings is still at initial levels. Several ICT-related courses have been established, for instance under the Master's programme on Mathematics and Computer Science of the University of Antananarivo or at the Higher Polytechnic Institute of Madagascar, and a seminar on cybercrime is offered to law students at the University of Antananarivo. However, no dedicated degree programmes have been established on specialised topics, such as information security, network security or cryptography, which could form the basis for deploying cybersecurity courses, before offering dedicated degree programmes on cybersecurity.

Even though some course instructors could be drawn from experienced organisations, such as the ISOC chapter of Madagascar or NIC-MG, which manages the national Internet country code top-level domain (ccTLD), a key obstacle of developing more specialised degrees at universities is the lack of training for educators. Another impediment is the uncertainty regarding the best approach towards integrating cybersecurity into national curricula. Participants were keen to learn about existing models and best practice to effectively develop and deploy cybersecurity courses and degree programmes in Madagascar. Linking industry and academia to develop cybersecurity-related educational offerings was additionally raised as an important step to ensure that the courses offered by universities meet the needs of the market.

Alongside the development of cybersecurity education, participants emphasised the strong link to national awareness-raising. In order to enhance the building of knowledge and skills across the country, political commitment is needed and awareness-raising efforts that are practical and pragmatic, while recognising the significance of cybersecurity beyond technical aspects, need to be implemented in conjunction with educational offerings.

F 3.3: Framework for Professional Training

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

Stage: Start-up to Formative

Start-up Formative Established Strategic Dynamic

Cybersecurity training offerings in Madagascar are still very limited. The main providers of training on specialised topics, such as network security or machine-to-machine communication, are the ISOC chapter of Madagascar and InATA, which has developed online training courses for distant learning that will be available from late 2016. The majority of these courses target IT professionals. However, according to participants, awareness of available trainings is very low and interested professionals would rather pursue training offerings in other countries.

While the national demand for training and certifications is still relatively low, trainings that are provided in an *ad hoc* manner have been received very positively and uptake was high, which indicates increasing interest in cybersecurity trainings.

As training offerings are gradually expanded at the national level, knowledge transfer between employees is an effective and resource-efficient way of enhancing the skills base.

Recommendations

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

Awareness Raising

Cybersecurity awareness raising efforts are limited to uncoordinated *ad hoc* initiatives. There are no current efforts to raise the awareness of executive staff in any sector. In order to enhance the level of capacity regarding cybersecurity awareness-raising, we recommend the following actions:

- **R3-1:** Develop a national cybersecurity awareness raising programme with specified target groups, focusing on the most vulnerable users.
- **R3-2:** Engage relevant stakeholders from public and private sectors in the development and delivery of the awareness raising programme.
- **R3-3:** Develop a dedicated awareness raising programme for executive managers within the public and private sectors.

Framework for Education

No specific cybersecurity courses are offered in Madagascar, nor is there a sufficient cadre of trained instructors to conduct these courses. Uncertainty regarding the most effective approach towards integrating cybersecurity in national curricula and a lack of coordination between industry and academia represent obstacles of enhancing capacity of this factor. Regarding the development of cybersecurity education, we recommend the following actions:

- **R3-4:** Develop degree programmes on specialised areas, such as information security, network security and cryptography and integrate cybersecurity modules in these programmes. Use best practices from within and beyond the region.

- **R3-5:** Create cybersecurity education programmes for instructors to ensure that skilled staff is available to teach newly formed cybersecurity courses.
- **R3-6:** Allocate additional resources to cybersecurity education for public universities.
- **R3-7:** Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy.

Framework for Professional Training

Some *ad hoc* trainings are offered in Madagascar, but the understanding of cybersecurity training demand and supply is limited. There is also a need for coordination between training providers and academic partners to ensure a harmonised approach towards education and training offerings. Knowledge transfer within organisations is uncommon. The following recommendations are proposed to enhance the capacity within professional training:

- **R3-8:** Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals.
- **R3-9:** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.
- **R3-10:** Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

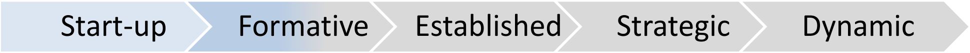
Dimension 4: Legal and Regulatory Frameworks

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.

F 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, intellectually property, substantive and procedural cybercrime legislation.

Stage: Start-up to Formative



In 2014, several laws that regulate cybersecurity and related topics have been adopted in Madagascar. Relevant laws include: Law No. 2014-006 on the Fight Against Cybercrime *(Loi n°2014-006 sur la lutte contre la cybercriminalité)*, Law No. 2014-024 on Electronic Transactions *(Loi n°2014-024 sur les transactions électroniques)*, Law No. 2014-025 on Electronic Signature *(Loi n°2014-025 sur la signature électronique)*, Law No. 2014-026 Establishing the General Principles Relating to the Dematerialisation of Administrative Procedures *(Loi n°2014-026 fixant les principes généraux relatifs a la dématérialisation des procédures administratives)*, and Law No. 2014-038 on the Protection of Personal Data *(Loi n° 2014-038 sur la protection des données à caractère personnel)*. While these laws build a broad framework for cybersecurity in the country and several stakeholders, including ARTEC, have been consulted in the development of legislation, participants identified the need to amend and supplement the legislative framework, as some aspects, such as child online protection or digital evidence, are not sufficiently addressed. Moreover, enforcement and implementation of the new legislation was raised as a concern by many participants.

While Madagascar has not adopted specific legislation on human rights online, it has acceded to or ratified several international instruments on human rights, including the *International Covenant on Civil and Political Rights*, the *Convention Against Torture and Other Cruel, Inhuman and Degrading Treatment or Punishment*, the *Convention on the Elimination of All Forms of Discrimination against Women*, and the *African Charter on Human and Peoples' Rights*.[5] Several key human rights principles are codified in the Constitution of the Republic of

[5] See http://www.claiminghumanrights.org/madagascar.html.

Madagascar, 2010 (*Constitution de la IVe République*), such as the right to privacy (Article 13), right to information (Article 11), freedom of expression (Article 10) and freedom of opinion (Article 10). However, according to participants, the enforcement of these provisions, in particular in cyberspace, are insufficient and there is a need for supplementary legislation to address human rights online. None of the participant was aware of any court cases that applied the general human rights provisions to offences conducted online and participants agreed that there is a lack of knowledge among prosecutors and judges regarding the application of human rights provisions online.

With regards to data protection, Law No. 2014-038 on the Protection of Personal Data *(Loi n° 2014-038 sur la protection des données à caractère personnel)* sets a comprehensive framework for the collection, storage, processing and transfer of personal data, including the establishment of an independent commission to monitor the protection of personal data across Madagascar. However, participants expressed doubts regarding the enforcement and enforceability of the new law, as there have not been any actual cases applying the new provisions. Criminal justice officials rather try to extend conventional law in cases of violations of data protection, even though these laws do not address digitally stored data. Moreover, participants criticised gaps in Law No. 2014-038, as data theft and online hacking are not explicitly addressed.

In contrast to the general data protection framework, no similar law has been established for the protection of children. The only specific provision is found in the recent Law No. 2014-006 on the Fight Against Cybercrime *(Loi n°2014-006 sur la lutte contre la cybercriminalité)*, which establishes the production, procurement and distribution of child pornography through electronic means as crimes in Article 22. Other aspects of child online protection, such as preventing children from accessing harmful online content, the protection of children's rights online, the protection from online grooming or cyber bullying, etc., have not yet been addressed. While some agencies have started to place emphasis on child online protection, in particular the United Nations International Children's Emergency Fund (UNICEF), a robust legislative framework is essential to ensure the effective protection of children online.

Similarly, there is no comprehensive legal framework that regulates consumer protection online, which is similar to many developing and transition economies globally.[6] While general consumer protection provisions have been established, participants agreed that these are not applicable to the online space and e-commerce. Some participants indicated that a draft law is in development to address the protection of consumer in online transactions. However, most participants were not aware of the draft legislation and some called for a dedicated cybersecurity law instead that would inter alia protect consumers from online fraud.

While general laws are in place, intellectual property legislation is not applicable to online content and the development of such provisions are not yet being discussed.

[6] See http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx.

Finally, substantive cybercrime provisions are contained in Law No. 2014-006 on the Fight Against Cybercrime *(Loi n°2014-006 sur la lutte contre la cybercriminalité)*. The law criminalises different types of offences, distinguishing between offences against the confidentiality, integrity and availability of computer data and systems (such as illegal access to computer systems and data, data and system interference, illegal interception and production, possession and distribution of computer misuse devices) and offences that cause harm to persons (such as online harassment, defamation, identify theft and child pornography). It also lays out obligations of Internet service providers. However, the law does not specify investigative powers for law enforcement in investigations involving digital evidence. As a result, police officers rely on conventional procedures to investigate cybercrime. Madagascar has not yet signed the *African Union Convention on Cyber Security and Personal Data Protection* and is not party to any other multilateral cybercrime agreement. Entering into bilateral or multilateral agreements would facilitate international cooperation to combat cybercrime by setting a framework for mutual legal assistance and extradition, as well as informal cooperation channels.

Overall, the legislative framework regulating cybersecurity and related topics is still in the start-up to formative stages of development, as recently adopted legislation does not cover all aspects of cybersecurity, such as consumer protection online, digital evidence regulations, human rights protection online, etc., and is not yet sufficiently enforced. In order to enhance capacity of this factor, review participants have indicated that the 2014 legal framework requires revision, which involves cooperation with all relevant stakeholders.

F 4.2: Criminal Justice System

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

Stage: Start-up

Start-up
Formative
Established
Strategic
Dynamic

Across the criminal justice system, capacities are at initial stages of development in Madagascar. While there is no specialised cybercrime unit in the law enforcement structure, some dedicated staff members of the National Police and Gendarmerie work on cybercrime. However, only very few police officers have received specialised training and participants emphasised a lack of technical equipment. In lieu of regulation on digital chain of custody, police officers largely rely on traditional measures and chain of custody principles rather than applying specialised methods.

The capacities of prosecutors to handle cybercrime cases and cases involving digital evidence was considered to be even more limited. Only very few cybercrime cases have been brought to the courts and prosecutors do not receive training on cybercrime or digital evidence.

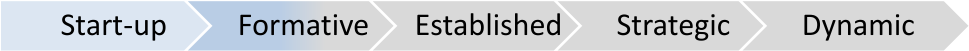
Similarly to prosecutors, the capacity of courts to handle cybercrime cases was perceived as low and no specialised training is available to judges.

These limited levels of capacity in handling cybercrime cases could potentially lead to ineffective investigations, prosecutions and convictions, which would allow cybercriminals to remain unpunished and continue their criminal conduct.

F 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime

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

Stage: Start-up to Formative



The need to establish informal and formal cooperation mechanisms, both domestically and across borders, has not yet been widely recognised in Madagascar, as cybercrime has only recently emerged as an issue of concern and there have not been many major cases that were brought before the courts. Among the different available cooperation channels, the engagement between law enforcement agencies and ISPs is most advanced. However, this engagement is typically mandated by the court in the course of securing evidentiary materials for specific cases involving digital evidence. INTERPOL was further emphasised as an important channel to facilitate cross-border cooperation. However, these informal relationships have not been institutionalised and are *ad hoc* in nature.

The establishment of a formal mechanism that ensures mutual legal assistance and extradition in cybercrime cases is essential to effectively prosecute. Cooperation channels that have been established to counter corruption could serve as a role model in this context, as there are institutionalised and routinized links between organisations, such as the Bureau Indépendant Anti-Corruption, Gendarmerie, police departments, etc., which could be expanded, adapted or replicated to facilitate cooperation to combat cybercrime.

Recommendations

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

Legal Frameworks

A broad legal framework to address cybersecurity and related issues was established in 2014 and 2015 with the adoption of several new laws on cybercrime, electronic transactions, electronic signature and personal data, among others. However, these laws do not address all relevant issues and require revision. Moreover, enforcement is insufficient. Therefore, in order to improve maturity to a higher stage, we recommend the following:

- **R4-1:** Revise and adapt the established legislative framework addressing cybersecurity, cybercrime and data protection. Develop new legislative provisions on human rights online, child online protection, consumer protection and intellectual property online.
- **R4-2:** Dedicate resources to ensure full enforcement of existing cybersecurity laws and monitor implementation.
- **R4-3:** Develop and adopt legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime.
- **R4-4:** Consider joining regional cybercrime instruments.

Criminal Justice System

The capacity of law enforcement officers, prosecutors and courts is at initial levels of development. While some members of the police have received training on cybercrime, these trainings have not been institutionalised and are not available for prosecutors and judges. Moreover, technical and financial resources are not sufficient to effectively investigate cybercrime. In order to enhance the capacity of the criminal justice system, we recommend the following:

- **R4-5:** Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.
- **R4-6:** Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence.

Formal and Informal Cooperation Frameworks to Combat Cybercrime

Formal and informal channels of cooperation to combat cybercrime have not yet been institutionalised domestically and across borders. Existing cooperation via INTERPOL or between police and ISPs is limited and *ad hoc*. In order to fully move to the formative stage of maturity in this factor, we recommend the following:

- **R4-7:** Establish formal international cooperation mechanisms, including mutual legal assistance and extradition, to combat cybercrime.
- **R4-8:** Strengthen informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders. Consider experiences made in other areas, such as anti-corruption cooperation.

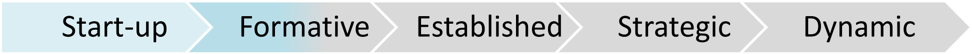
Dimension 5: Standards, Organisations, and Technologies

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.

F 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 to Formative



Start-up Formative Established Strategic Dynamic

There is currently no coordinated effort to develop a nationally agreed baseline of cybersecurity related standards and good practices in Madagascar. Among telecommunications operators, some organisations have begun to implement international standards, such as the ISO 27001, but there is no synchronisation across the sector. Access control was highlighted by multiple companies as an important cybersecurity measure that is standardised within organisations. Generally, national operators with an international parent company are further advanced in applying cybersecurity standards, as they are under obligations determined by the parent organisation. There is also no mechanism to establish synergies between government and private sector to harmonise approaches towards cybersecurity standards implementation. Hence, procedures and policies are developed and applied in silos.

Similar observations were made with regards to procurement and software development standards. While some procedures are in place to ensure cybersecurity in procurement practices in the public sector, these are limited to the institutional level and are not harmonised with the private sector. Even though the telecommunications sector has started to place emphasis on cybersecurity standards compliance, participants stated that small- and medium-sized enterprises (SMEs) are mostly not worried about adopting and implementing standards. However, there are some exceptional cases in which telecommunications operators have been approached sporadically by smaller companies to assist with adopting cybersecurity standards or procedures.

The discussions indicated that ARTEC and the main telecommunications companies could take a lead in facilitating the broader adoption and implementation of cybersecurity standards, as well as promoting coordination and harmonisation across sectors.

F 5.2: Internet Infrastructure Resilience

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

Stage: Start-up

Start-up Formative Established Strategic Dynamic

Review participants raised several concerns regarding the resilience of Internet infrastructure. Even though Internet infrastructure is established and is continuously expanding, Internet penetration is limited as costs are very high[7] and service is not yet reliable. Internet downtime and interruptions, often caused by power outages, are frequent. Security of Internet infrastructure was raised as a concern by major telecommunications operators, but SMEs and the general market often lack awareness of cybersecurity. Participants emphasised the need to make the national backbone more resilient.

F 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

Start-up Formative Established Strategic Dynamic

While the quality and performance of deployed software was an issue of concern to participants, the diversity of software available across Madagascar was perceived as an obstacle to effective monitoring and quality assessment. Overall, policies on software deployment, maintenance and update are not common in private and public sectors. Software quality is not monitored and there is no catalogue of secure software platforms and applications. Participants noted that there is no organisation that collects data on the kinds of software that are deployed in the country, and some participants referred to examples of the use of counterfeit software. ARTEC could take the lead in identifying this information and making it available to the wider public to promote the use of more secure software solutions.

[7] For example, high-speed Internet access (from 512 kbit/s) costs USD 125, or 250% of the average monthly wage.

F 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

Start-up | Formative | Established | Strategic | Dynamic

The use of technical security controls in Madagascar varies across sectors and organisations. Participants agreed that ISPs routinely deploy firewalls to protect the networks. Within some organisations, firewall rulesets and anti-malware solutions are developed in-house; in others, technical security controls are provided by the international parent company or purchased externally. However, the use of technical security controls outside of the telecommunications sector is inconsistent and sporadic rather than routine. While ISPs try to protect their networks, they do not yet offer anti-malware software or other technical security solutions to their customer and do not encourage users to take proactive measures to secure their personal devices. Basic Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS), are rarely deployed.

Generally, the level of understanding and deployment of security controls by public and private sectors, and users, is low. Raising awareness of security controls and promoting their use among all sectors of the country is an important step in enhancing the capacity within this factor.

F 5.5: Cryptographic Controls

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

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

Encryption has recently emerged as an issue of concern relating to cyber-incidents in Madagascar. For instance, after e-mail accounts of the Gendarmerie were hacked, new procedures were put in place that require encryption of all e-mail attachments. Participants from the defence sector stated that the need for encryption is recognised, but that the implementation has not yet commenced. On the other hand, within the telecommunications sector, data are routinely encrypted at rest, but not in transit. Overall, the capacity to deploy cryptographic controls across sectors is still very low and recognition of the need for encryption has only just begun. Broader discussion and awareness raising across all sectors of society would help facilitate the maturity of this capacity.

F 5.6: Cybersecurity Marketplace

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

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

No domestic market for cybersecurity technologies and cybercrime insurance products has yet been developed in Madagascar. While international providers offer a range of cybersecurity products for domestic use and some domestic companies have started to develop solutions, such as firewall rulesets, for internal use, there are no domestic commercial cybersecurity products or cybercrime insurance offerings on the Malagasy market.

F 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

Start-up | Formative | Established | Strategic | Dynamic

No responsible disclosure policy or framework has been established in the public or private sectors. Even though vulnerabilities are an increasing concern in the telecommunications sector, they are perceived as confidential commercially valuable information and, as such, organisations prioritise solving detected issues internally and do not share information with other operators or across sectors. Several ISPs have developed policies and guidelines that determine the procedures to be followed once a vulnerability has been identified. However, these policies do not extend beyond the organisational borders.

In some cases that cannot be solved in-house and require external assistance, such as in large-scale SIM box fraud cases, ISPs turn to ARTEC for support. Given its coordinative role, ARTEC may be in a suitable position to establish and promote a responsible disclosure framework in Madagascar.

Recommendations

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

Adherence to Standards

No coordinated effort to adopt and implement cybersecurity standards can be evidenced in Madagascar. There is also no synergy between government and private sector to harmonise approaches towards cybersecurity standards. Different organisations adhere to different standards according to their needs or obligations handed down by parent companies. Procurement and software development security standards are not yet widely adopted. Therefore, the following actions are recommended:

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

Internet Infrastructure Resilience

Internet infrastructure is not yet reliable and affordable. Internet downtimes and interruptions are frequent. The following recommendations are provided to increase the maturity of national Internet infrastructure resilience:

- **R5-4:** Increase reliability of Internet infrastructure and expand the national programme for infrastructure development.
- **R5-6:** Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors.
- **R5-7:** Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.

Software Quality

Software quality is not monitored and there is no catalogue of secure software platforms and applications. Policies and processes regarding updates of software applications have not yet been formulated. Therefore, in order to improve maturity to a higher stage, we recommend the following:

- **R5-8:** Develop a catalogue of secure software platforms and applications within the public and private sectors.
- **R5-9:** Develop policies and processes on software updates and maintenance.
- **R5-10:** Gather and assess evidence of software quality deficiencies regarding its impact on usability and performance.

Technical Security Controls

The deployment of technical security controls by users, and the public and private sectors is limited. ISPs prioritise securing their own networks, including the use of firewalls and anti-malware software, but do not provide solutions or guidance for end-users. Basic Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are rarely deployed. In order to enhance the capacity of this factor, we recommend the following:

- **R5-11:** Promote user understanding of the importance of anti-malware software and network firewalls.
- **R5-12:** Encourage ISPs to establish policies for technical security control deployment as part of their services.

Cryptographic Controls

Cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and data in transit have been identified as a concern but are not yet deployed consistently within the government, private sector and the general public. Therefore, in order to improve maturity to a higher stage, we recommend the following:

- **R5-13:** Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines.
- **R5-14:** Raise public awareness of secure communication services, such as encrypted/signed emails.

Cybersecurity Marketplace

Technologies are not produced domestically, but imported. Cybercrime insurance is neither available, whether domestically or from the region, nor is it a topic of public discussion. Therefore, we recommend:

- **R5-15:** Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development.
- **R5-16:** Promote sharing of information and best practices among organisations, to explore potential cybercrime insurance coverages.

Responsible Disclosure

No responsible disclosure policy or framework in public and private sector has been established. In order to enhance the capacity of this factor, we recommend the following:

- **R5-17:** Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledge report.
- **R5-18:** Encourage sharing of technical details of vulnerabilities among critical infrastructure and ISPs.

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 comprehensive. We note that participants generally refrained from stretching to claim higher levels of maturity than could be evidenced, and so we are confident that the assessments made are sound.

This was the thirteenth country review that we have supported directly, and the fourth review in the African region. It was the second review that used the revised edition of the CMM as a basis and, as such, provided useful input regarding the impact of changes made to the model.

Madagascar has commenced the process of developing different aspects of cybersecurity capacity across all dimensions, including through developing a broad legal framework and the gradual expansion of cybersecurity training offerings. These efforts will set the foundations for more advanced capacity in the future. We hope that this review will offer useful insights to Madagascar and that our recommendations on how to increase cybersecurity capacity will contribute to the on-going work on enhancing cybersecurity capacity across all five dimensions of the CMM.

Appendix I: Review Results

Dimension	Capacity Factor	Stage of Maturity	Brief Description	References	Recommendations
Dimension 1 Cybersecurity Policy and Strategy	**F 1.1 National Cybersecurity Strategy**	**Start-up**	The drafting of a national cybersecurity strategy has not yet begun. Responsibilities for enhancing cybersecurity capacity across the country remain dispersed and often uncoordinated among different organisations.		• **R1-1:** A formal decision by the Government of Madagascar to embark upon a National Cybersecurity Strategy. This document should set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. The strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives. • **R1-2:** Allocate budget and assign a government agency to oversee the implementation of the National Cybersecurity Strategy, taking into account existing roles and responsibilities. • **R1-3:** Design and disseminate coordinated cybersecurity programmes. • **R1-4:** Strengthen and promote inter-departmental cooperation in cybersecurity.
	F 1.2 Incident Response	**Start-up**	There is no national CSIRT and no central structure to provide national incident response. Incidents are not categorised or recorded.		• **R1-5:** Continue work towards the development of a national CSIRT/CIRT with clear processes and defined roles and responsibilities, • **R1-6:** Categorise and record national-level cyber incidents in a central

			Communication channels between actors remain reactive, *ad hoc* and inconsistent in incident response, impeding effective incident management.		registry, possibly hosted by the national CSIRT/CIRT. • **R1-7:** Draft legislation, which allocates mandates to the national CSIRT/CIRT. • **R1-8:** Develop coordination and information/cybersecurity threat sharing mechanisms between the private and the public sector, as well as within the cybersecurity community at national, regional and international levels. • **R1-9:** Appoint and publicize a national-level lead to ensure reporting of incidents and promote reporting.
	F 1.3 Critical Infrastructure (CI) Protection	**Start-up**	No central list of CI assets has been identified. Interaction between government ministries and owners of critical assets on cybersecurity is limited. A cybersecurity operational strategy or plan to manage and mitigate cybersecurity incidents in case of a coordinated cyber-attack on CI is not in place. Incident response by CI is uncoordinated, without a formal cyber response plan or official mandate. Risk management exercises and drills specific to cybersecurity are not conducted at a national level.		• **R1-10:** Develop and disseminate a list of Critical Infrastructure (CI) assets with identified risk-based priorities. • **R1-11:** Establish a mechanism for regular vulnerability disclosure and information sharing between the public and private sector. • **R1-12:** Establish information protection and risk management procedures and processes, supported by adequate technical security solutions, which inform the development of an incident response plan. • **R1-13:** Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CI operators.
	F 1.4 Crisis Management	**Start-up**	While national crisis management exercises are held periodically with	National Bureau of Risk Management and Disaster	• **R1-14:** Conduct a needs assessment of measures that require testing with

			institutionalised evaluation mechanisms, cybersecurity elements have not yet been integrated into these exercises.	Management *(Le Bureau National de Gestion des Risques et Catastrophes - BNGRC)* http://www.bngrc-mid.mg/	consideration of a simple exercise scenario. • **R1-15:** Conduct compromised communication scenarios and exercises to test emergency response assets interoperability and function effectively. • **R1-16:** Evaluate the exercises and feed the findings back into the decision-making process.
	F 1.5 Cyber Defence Consideration	**Start-up**	Madagascar does not have a specific national cyber Defence policy or strategy. Operational cyber Defence capacity has not yet been developed and there is no coordination or communication in the security sector on cybersecurity threats.		• **R1-17:** Develop a cyber Defence component in the national security strategy, taking into consideration identified threats to national security in cyberspace. • **R1-18:** Develop a communication and coordination framework for cyber Defence. • **R1-19:** Expand coordination in response to malicious cyber-attacks on military information systems and critical infrastructure. • **R1-20:** Conduct continuous review of the evolving threat landscape in cybersecurity to ensure that cyber Defence policies continue to meet national security objectives.
	F 1.6 Communications Redundancy	**Start-up to Formative**	Basic sectoral and organisational communications redundancy has been established. However, coordination is limited.		• **R1-21:** Allocate appropriate resources not solely to such activities as hardware integration, technology stress testing, personnel training and crisis simulation drills, but also to ensuring that redundancy efforts are appropriately communicated to relevant. • **R1-22:** Link all emergency response

					assets into a national emergency communication network with isolated but accessible backup systems. • **R1-23:** Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.
Dimension 2 Cyber Culture and Society	**F 2.1 Cybersecurity Mind-set**	**Start-up to Formative**	A cybersecurity mind-set is adopted inconsistently and not engrained across society. Cybersecurity is a concern, but mainly for IT professionals. Within some large private sector organisations an increasing understanding of cybersecurity threats and risks is developing. However, most private sector entities, in particular SMEs, do not recognise the need for cybersecurity yet. Users are generally unaware of cybersecurity threats.		• **R2-1:** Enhance efforts at all levels of government to promote understanding of risks and threats, but also to design systems that enable users across society to more easily embed secure practices into their everyday use of the Internet and online services. • **R2-2:** Promote the sharing of information on incidents and best practices among organisations to promote a proactive cybersecurity mind-set. • **R2-3:** Promote prioritisation of risk and threat understanding for private sector entities by identifying high-risk practices. • **R2-4:** Develop programmes and materials to train the public and improve cybersecurity practices.
	F 2.2 Trust and Confidence on the Internet	**Start-up to Formative**	Trust in online services is identified as a concern. Users do not have enough knowledge regarding safe online practises and the Internet is often used with “blind” trust. E-government services are under		• **R2-5:** Develop campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content. • **R2-6:** Expand e-government services with recognition of the need for the application of security measures to

			development, but they are not yet secure and reliable. No e-commerce services have been established.		promote trust in e-services. - **R2-7:** Encourage the development of e-commerce services, while emphasising the need for security.
	F 2.3 User Understanding of Personal Information Protection Online	**Start-up**	Stakeholders within the public and private sectors have minimal knowledge about how personal data are handled online, and they do not believe that adequate measures are in place to protect their information online. Awareness and discussion regarding the protection of personal information online are limited.		- **R2-8:** Establish programmes to raise user awareness of online risks and measures available to be safe online and protect privacy. - **R2-9:** Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.
	F 2.4 Reporting Mechanisms	**Start-up to Formative**	There is no centrally coordinated reporting mechanism for cybersecurity incidents in Madagascar. Channels to report online child abuse have been established, but do not extend to other types of cybercrime.		- **R2-10:** Establish a central mechanism that allows citizens to report all types of cybercrime. Use experiences gathered through the child abuse hotlines managed by UNICEF and ISPs. - **R2-11:** Raise awareness about existing reporting channels among the wider public.
	F 2.5 Media and Social Media	**Start-up to Formative**	Media rarely cover information about cybersecurity or report on issues relating to cybercrime or other incidents. Social media are not currently used to communicate and disseminate messages on cybersecurity.		- **R2-12:** Encourage media content providers to disseminate information on good cybersecurity practice, which could stimulate social media discussions on this topic. - **R2-13:** Develop programmes to raise awareness among media and social media providers and actors on cybersecurity issues, for instance through a dedicated cybersecurity awareness month or dedicated sites on this topic.

Dimension 3 Cybersecurity Education, Training and Skills	**F 3.1 Awareness Raising**	**Start-up**	Cybersecurity awareness raising efforts are limited to uncoordinated *ad hoc* initiatives. There are no current efforts to raise the awareness of executive staff in any sector.		• **R3-1:** Develop a national cybersecurity awareness raising programme with specified target groups, focusing on the most vulnerable users. • **R3-2:** Engage relevant stakeholders from public and private sectors in the development and delivery of the awareness raising programme. • **R3-3:** Develop a dedicated awareness raising programme for executive managers within the public and private sectors.
	F 3.2 Framework for Education	**Start-up**	While computer science is offered as a module at some universities, no specific cybersecurity courses are offered in Madagascar, nor are there trained instructors to conduct these courses. Coordination for cybersecurity education between the universities and public/private sectors is limited.	University of Antananarivo *(Université d'Antananarivo)* http://www.univ-antananarivo.mg/Master-en-Droit Higher Polytechnic Institute of Madagascar (*Institut Supérieur Polytechnique de Madagascar*) http://ispm-edu.com/	• **R3-4:** Develop degree programmes on specialised areas, such as information security, network security and cryptography and integrate cybersecurity modules in these programmes. Use best practices from within and beyond the region. • **R3-5:** Create cybersecurity education programmes for instructors to ensure that skilled staff is available to teach newly formed cybersecurity courses. • **R3-6:** Allocate additional resources to cybersecurity education for public universities. • **R3-7:** Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy.
	F 3.3 Framework for Professional Training	**Start-up to Formative**	*Ad hoc* trainings are offered in Madagascar, but the understanding of cybersecurity training needs is restricted. There is also a need for	Institute of Arts and Advanced Technologies *(Institut des Arts et des*	• **R3-8:** Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT

			coordination between training providers and academic partners to ensure a harmonised approach towards education and training offerings. Knowledge transfer within organisations is uncommon.	*Technologies Avancées - InATA)* http://www.inata.org/formations/	professionals. • **R3-9:** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools. • **R3-10:** Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.
Dimension 4 Legal and Regulatory Frameworks	**F 4.1 Legal Frameworks**	**Start-up to Formative**	A cybersecurity legal framework was established in Madagascar in 2014 and 2015. However, these laws require revision and have not yet been fully implemented.	Constitution of the Republic of Madagascar, 2010 (*Constitution de la IVe République*) Law No. 2014-006 on the Fight Against Cybercrime *(Loi n°2014-006 sur la lutte contre la cybercriminalité)* Law No. 2014-024 on Electronic Transactions *(Loi n°2014-024 sur les transactions électroniques)* Law No. 2014-025 on Electronic Signature *(Loi n°2014-025 sur la signature électronique)* Law No. 2014-026 Establishing the General Principles Relating to the	• **R4-1:** Revise and adapt the established legislative framework addressing cybersecurity, cybercrime and data protection. Develop new legislative provisions on human rights online, child online protection, consumer protection and intellectual property online. • **R4-2:** Dedicate resources to ensure full enforcement of existing cybersecurity laws and monitor implementation. • **R4-3:** Develop and adopt legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime. • **R4-4:** Consider joining regional cybercrime instruments.

				Dematerialisation of Administrative Procedures *(Loi n°2014-026 fixant les principes généraux relatifs a la dématérialisation des procédures administratives)* Law No. 2014-038 on the Protection of Personal Data *(Loi n° 2014-038 sur la protection des données à caractère personnel)* Available at http://www.assemblee-nationale.mg/?post_type=loi	
	F 4.2 Criminal Justice System	**Start-up**	Law enforcement officers have limited capacity to investigate cybercrime in accordance with domestic law, however this is minimal. Prosecutors and courts are not trained and do not have the capacity to prosecute and preside over cybercrime cases. Human, financial and technical resources of criminal justice actors are lacking.		• **R4-5:** Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody. • **R4-6:** Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence.
	F 4.3 Formal and Informal	**Start-up to Formative**	Informal channels of cooperation are sporadically used to combat		• **R4-7:** Establish formal international cooperation mechanisms, including

	Cooperation Frameworks to Combat Cybercrime		cybercrime domestically and across borders. Formal cooperation mechanisms have not been established.		mutual legal assistance and extradition, to combat cybercrime. • **R4-8:** Strengthen informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders. Consider experiences made in other areas, such as anti-corruption cooperation.
Dimension 5 Standards, Organisations and Technologies	**F 5.1 Adherence to Standards**	**Start-up to Formative**	No coordinated effort to adopt and implement cybersecurity standards can be evidenced in Madagascar. There is also no synergy between government and private sector to harmonise approaches towards cybersecurity standards. The implementation of standards in procurement and software development practices is *ad hoc* and uncoordinated.		• **R5-1**: Establish a programme to strengthen government's capacity to adapt or adopt international standards in order to acquire a baseline in the context of organisational cybersecurity. • **R5-2:** Promote adoption of international IT standards, in particular during procurement and software development. • **R5-3:** Promote the awareness and implementation of standards among SMEs.
	F 5.2 Internet Infrastructure Resilience	**Start-up**	Internet infrastructure is not yet reliable and affordable. Internet downtimes and interruptions are frequent.		• **R5-4:** Increase reliability of Internet infrastructure and expand the national programme for infrastructure development. • **R5-6:** Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors. • **R5-7:** Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.

	F 5.3 Software Quality	**Start-up**	Software quality is not monitored and there is no catalogue of secure software platforms and applications. Policies and processes regarding updates of software applications have not yet been formulated.		• **R5-8:** Develop a catalogue of secure software platforms and applications within the public and private sectors. • **R5-9:** Develop policies and processes on software updates and maintenance. • **R5-10:** Gather and assess evidence of software quality deficiencies regarding its impact on usability and performance.
	F 5.4 Technical Security Controls	**Start-up**	The deployment of technical security controls by users, public and private sectors is limited. ISPs prioritise securing their networks, including through firewalls and anti-malware software, but do not provide solutions or guidance for end-users. Basic Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are rarely deployed.		• **R5-11:** Promote user understanding of the importance of anti-malware software and network firewalls. • **R5-12:** Encourage ISPs to establish policies for technical security control deployment as part of their services.
	F 5.5 Cryptographic Controls	**Start-up**	Cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and data in transit have been identified as a concern but are not yet deployed consistently within the government, private sector and the general public.		• **R5-13:** Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines. • **R5-14:** Raise public awareness of secure communication services, such as encrypted/signed emails.
	F 5.6 Cybersecurity Marketplace	**Start-up**	There is no domestic cybersecurity marketplace. Foreign technologies are being solely deployed and no security products are produced domestically.		• **R5-15:** Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development. • **R5-16:** Promote sharing of information

			The need for developing a cybercrime insurance market was not yet identified at a national level.		and best practices among organisations, to explore potential cybercrime insurance coverages.
	F 5.7 Responsible Disclosure	**Start-up**	No responsible disclosure policy or framework in public and private sector has been established.		• **R5-17:** Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledge report. • **R5-18:** Encourage sharing of technical details of vulnerabilities among critical infrastructure and ISPs.

Global
Cyber Security
Capacity Centre

ITU

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD

DEPARTMENT OF
COMPUTER
SCIENCE

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

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