RESEARCH ICT AFRICA

Policy Brief 1: Africa Digital Policy

October 2018, Mauritius

Collaborative Cybersecurity: the Mauritius case

- **Collaborative approaches to national cybersecurity strategies benefit from adaptability, transparency, and trusted information-sharing among all participants.**
- **Cybersecurity collaborations should display both vertical** (e.g., between overseeing organisations and other stakeholders) **and horizontal** (e.g., between peer stakeholders) **interaction between and among stakeholders, be descriptive rather than prescriptive, and be sufficiently flexible in order to adapt alongside evolving cyber risks and technologies.**
- **Special steps must be taken to involve stakeholders who could find it difficult to participate or who are more vulnerable to cyber threats, including civil society organisations and marginalised communities.**
- **Collaboration should extend not only to public and private sector entities who own and control critical information infrastructure, but also stakeholders from other sectors** (e.g. the technical community, the banking and finance sectors, business process outsourcing, health, tourism, and energy sectors) **and not-for-profit stakeholder groups** (e.g. academia and civil society)**.**
- **Commercial interests should not be the main driver for private sector stakeholders to participate in collaborative cybersecurity efforts. Rather, the private sector should innovate and mitigate threats, building security into applications and systems along with the need for raising awareness.**

As access to broadband networks expands, countries' exposure to cyber risks also grows. In Africa, the increasing availability of broadband; relatively weak, poor or undeveloped cybersecurity strategies; cybersecurity and digital skill shortages; and a general lack of awareness of cyber risks and security measures are but some factors that make many developing countries more susceptible to cyber threat and harm. Perhaps more significantly, such threats qualify and limit the oft touted potential of information and communication technologies (ICTs) for development as expressed in, for example, the UN Agenda for Sustainable Development 2030.[1]

As broadband penetration and adoption rates increase, countries' exposure to cyber risks also grows

The scale, scope and pace of evolving cyber threats cannot be adequately addressed by governments alone and demand the involvement of other

[1] UNGA (2015). Resolution adopted by the General Assembly on 25 September 2015: Transforming our world: the 2030 Agenda for Sustainable Development (A/Res/70/1). New York: UNGA. Available at: www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.

stakeholders. Because ICT and critical infrastructure (CI) are often privately owned, private sector involvement is often a precondition for successful cybersecurity strategies. Critical information infrastructures (CII), more specifically, tend to be owned and operated by multinational corporations headquartered outside most countries' borders.

While governments can, for example, act as convenors and focal points of information, the private sector can supply resources and expertise that support and multiply government efforts, especially where state institutions are under-resourced. Recent examples have also shown that when governments hesitate to act in, for example, identifying a state aggressor, private companies can attribute state-sponsored intrusions whilst enabling government deniability, preventing diplomatic fallout.

One example is a strong early warning and incident response capability, which has to rely on well-functioning National/Governmental Computer Emergency Response Teams (CERTs). These bodies need to act as national catalysers of stakeholders' interests and capacity for public policy activities (including those related to information and alert-sharing systems reaching out to citizens and SMEs) and to engage in effective cross-border cooperation and information exchange.

While the sharing of information between stakeholders is crucial to cybersecurity and CI protection, parties might withhold sensitive information because of a lack of trust, the difficulty of correctly and quickly identifying a cyber incident as potentially threatening, commercial interest in withholding potential vulnerabilities from competitors, and/or reputational risk.

Why Mauritius?

The ITU's *Global Cybersecurity Index* ranks Mauritius as **first in Africa and sixth globally**

The International Telecommunications Union (ITU)'s 2017 *Global Cybersecurity Index* ranks Mauritius as first in Africa and sixth globally in terms of the country's commitment to cybersecurity.[2] The country scores particularly well in the *Index* where legal, technical and capacity-building are concerned.[3]

Mauritius has also become an increasingly active leader when it comes to promoting cybersecurity in the broader region. The Government has secured approval from the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) countries to establish a 'Regional Capacity Building Centre for Africa' to deal with cybersecurity, for example. The Centre is aimed at helping SADC countries formulate cybersecurity legislation and collaborate to combat cyber-attacks.[4]

[2] ITU (2017). *Global Cybersecurity Index 2017*. ITU: Geneva. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[3] The Government's IT Security Unit has been conducted cybersecurity training under the GLACY Project since 2013 and is still ongoing. So far, it has hosted 180 awareness sessions for some 2,000 civil servants in 32 government ministries and departments.

[4] ITWeb Africa (2018). *Mauritius champions a single cyber law for Africa*. Available at: http://www.itwebafrica.com/security/934-mauritius/244515-mauritius-champions-a-single-cyber-law-for-africa.

Examples of collaborative models for cybersecurity

Collaborative models for cybersecurity may vary in terms of objectives, scope, number and type of stakeholders involved, as well as governance structures and processes adopted in a particular context to address (a) specific concern(s).

Three common models often used in cybersecurity are:

Public Private Partnerships (PPP)

generally refer to situations when a private partner exclusively operates, maintains, and carries out the development of infrastructure or provides services of general economic interest to the state. Benefits include cost efficiency, the appropriate allocation of risks and responsibilities, better performance, diplomatic leverage, better business opportunities, and benefiting from resource sharing and respective strengths.

Public Private Initiatives (PPI)

span a broader set of relationships that are not upheld exclusively in one specific sector. While PPPs demand contractual obligations for viability, PPIs do not. For the ICT sector in general and cybersecurity in particular, PPIs are often more suitable than PPPs as they allow better interaction and flexibility between the public and private sectors.

Multistakeholder collaboration mechanisms

are popular in many fields where cross-border or international cooperation is sometimes needed, such as Internet governance, labour relations, and sustainable development. The participation of more stakeholders in governance can inject expertise and reflect a diversity of needs of those affected by these decisions, as well as encourage 'buy-in' from stakeholders for agreed actions.

The theory: cybersecurity as precondition for economic growth

The Government of Mauritius identified broadband as a potential key driver of economic growth and national competitiveness in 2012 and thus elaborated its *National Broadband Policy*[5] with the aim of leveraging the developmental opportunities introduced by broadband and ICTs and overcoming various challenges facing the electronic communications sector. At the same time, the Government realised that growing broadband access would come with increased exposure to cyber threats and harm. In this context, it was clear that the country

[5] Information and Communication Technologies Authority (ICTA) (2012). *National Broadband Policy (NBP2012).* Port Louis: Ministry of Information and Communication Technology. Available at: https://www.icta.mu/documents/nationalbroadbandpolicy2012.pdf.

would need to establish an adequate cybersecurity policy framework to complement the successful implementation of its N*ational Broadband Policy*.[6]

Mauritius' *National Cybersecurity Strategy 2014-2019*[7] was introduced with the aim of effectively protecting information systems and networks. The strategy document was drafted after a survey conducted on the state of information security in local businesses in October 2013. The strategy, which includes a policy formulation section, was designed with the aim of protecting individual users, enterprises and government bodies against cyber threats.

One of the goals in the strategy focuses on collaboration. It acknowledges that 'preparing sufficient cyber defence capabilities against cyber threats demands immediate, transparent and better coordinated actions from all stakeholders', be it from an individual user or collective perspective. A cybersecurity management framework is also required, it argues, to ensure that different stakeholders have reliable and real-time depictions of the country's cybersecurity status. The management structure thus hinges on a collaborative approach based on the core principle that information security preparedness for a country is the cornerstone of the national cybersecurity policy.

In practice: from narrow to broader collaboration

Mauritius moved from a more hierarchical, prescriptive PPP model to a more open and horizontal PPI model based on a collaborative 'interplay'

In 2017 and 2018, Research ICT Africa conducted a number of interviews with key stakeholders involved in cybersecurity in Mauritius to understand how the collaborative model could potentially serve as an example for other countries that are developing cybersecurity strategies and/or have committed to address cybersecurity through a collaborative approach. Some findings from the study include:

- In developing its national cybersecurity collaboration framework, Mauritius moved from a more hierarchical, prescriptive public-private partnership model (Phase 1 in Figure 1 below) to a more open and horizontal public-private initiative model based on a collaborative 'interplay' which included a wider range of stakeholders (Phase 2 Figure 1 below). The reason for this shift are summarised in Figure 1, but was generally because the original model was thought to overly restrictive and thus perceived as 'dysfunctional'.
- The broader, less rigid 'interplay' model (Phase 2 in Figure 1) included users as targets of public awareness campaigns from law enforcement agencies and the national Computer Emergency Response Team (CERT). However, it did not explicitly include mechanisms for users or civil society groups to participate in decision-making outside the normal democratic process of influencing

[6] United Nations Broadband Commission for Sustainable Development (2012). *Strategies for the promotion of broadband services and infrastructure: a case study on Mauritius*. Geneva: ITU. Available at: https://www.itu.int/ITU-D/treg/publications/BBD_MDG_Mauritius_Final.pdf.

[7] Republic of Mauritius (2014). *National Cyber Security Strategy 2014-2019*. Available at: http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf.

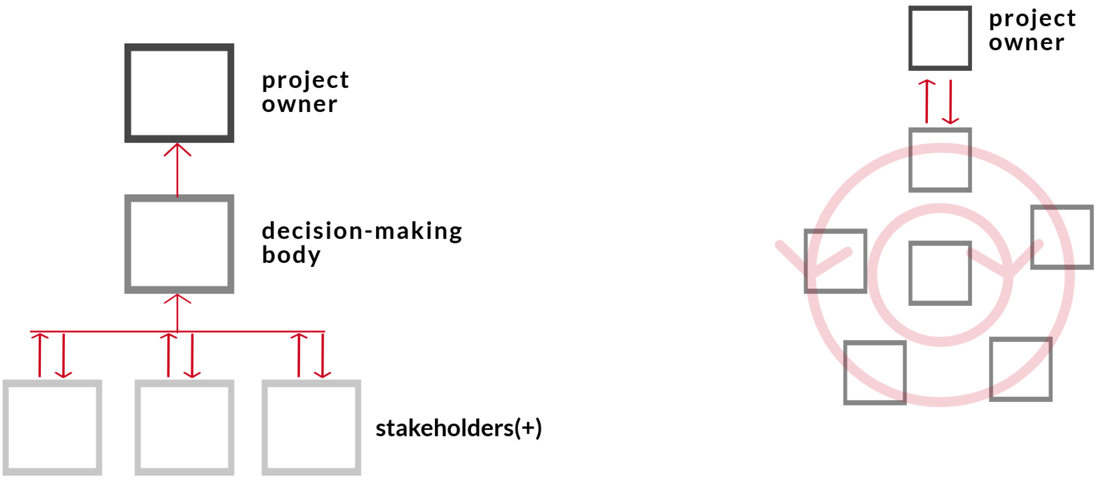
government. This could be an opportunity for greater stakeholder involvement in the future.

- Several stakeholders felt they could see benefits in an even more inclusive approach, which involved local banks as well as financial regulators; smaller businesses; and young IT professionals.

- The successful implementation of the PPI relied on information-sharing with the private sector and enhanced collaboration among stakeholders. While there are sound policy reasons for certain barriers to information-sharing (including privacy, commercial and national security concerns), these must be balanced with the importance of sharing information to support collective efforts to address cybercrime challenges – including actions related to cyber threats, vulnerabilities, breaches, protective measures and the adoption of best practices. The country's national Data Protection Act 2017[8] can be used to resolve some of these potential tensions.

PHASE I: PPP

PHASE II: PPI



PHASE I: PPP

- predefined roles
- hierarchical dependency
- prescriptive (lack of flexibility)
- some partners more powerful
- less information-sharing
- closed

PHASE II: PPI

- interactions, not predefined
- not hierarchical
- descriptive (more flexible)
- more equal; stakeholder buy-in
- robust information-sharing measures
- open

Figure 1: Depiction of the evolution of collaboration in Mauritius. Source: Adapted from Mauritius' National Cybercrime Strategy, 2017.

[8] Act No. 20 of 2017. Available at: http://dataprotection.govmu.org/English/Publications/Documents/Act%20No.%2020%20-%20The%20Data%20Protection%20Act%202017.pdf.

This summary draws from RIA's policy paper 1 - Series 6: Africa Digital Policy:

Van der Spuy, A., & Oolun, K. (2018). *Promoting cybersecurity through multistakeholder collaboration in Africa*. Research ICT Africa Working Paper, May 2018.

See the full paper at: www.researchictafrica.net

Contacts

Anri van der Spuy: avanderspuy@researchictafrica,net

Dr Enrico Calandro: ecalandro@researchictafrica.net

Dr Ian Brown: ibrown@researchictafrica.net

Acknowledgements

This policy brief is based on research conducted by Research ICT Africa in 2017/2018. We would like to acknowledge with gratitude Dr Krishna Oolun for developing the case on Mauritius, and Anri van der Spuy for developing the rest of the study. We also thank Dr Ian Brown and Dr Enrico Calandro for their valuable input and revisions. Any errors or omissions of course remain the authors' own.

IDRC CRDI

This report was made possible by the support received from Canada's international Development Research Centre (IDRC).