Submission to the Inquiry into the role and responsibilities of the Independent Communications Authority of South Africa in Cybersecurity

Attention:

Ms. Violet Letsiri

Senior Manager: Social Policy for ICT services

Tel: (011) 566 3715

Email: VLetsiri@icasa.org.za

30 November 2018

For further information please contact:

Enrico Calandro (PhD). Senior Researcher

ecalandro@researchictafrica.net

Telephone +27 21 447 6332. Fax +27 21 447 9529

Executive Summary

Research ICT Africa welcomes this opportunity to submit written comments on the *Inquiry into the role and responsibilities of the Independent Communications Authority of South Africa*, published in the *Government Gazette* on the 28 September 2018.

To that end, ICASA has published a discussion document soliciting the views of stakeholders on whether it should play a role in cybersecurity, with specific reference to:

- Private sector cooperation and industry regulation;
- Capacity building;
- Research and development; and
- Regulation of cybersecurity standards.

Research ICT Africa is a regional digital policy and regulation think tank active across Africa and the Global South. It conducts research on digital economy and society that facilitates evidence-based and informed policy making for improved access, use and application of ICT for social development and economic growth.

We thank ICASA for instituting a public process to determine roles and responsibilities of the regulator in cybersecurity, and to promote the idea that a safe and secure Internet is a matter of public interest which involves all South African stakeholders, including users, the public and private sectors, civil society organisations, the technical community and academia.

We make this submission in the public interest to ensure that the Internet, and access to it, can be a force for good in South Africa rather than becoming a tool which benefits some and leaves marginalized communities further behind.

As access to the Internet improves in South Africa, the country and its citizens' exposure to cyber threats also increases. Yet technology and cyberspace are changing faster than countries can legislate internally to keep them safe and secure. Part of the problem with defining and evaluating the roles and responsibilities of a regulator is that the South African Government has adopted a predominantly security-based approach to mitigating cyber-risks, which is expected to become unsustainable and costly. Furthermore, existing capability to deter cybercrime and monitor or pursue cybersecurity are insufficient and ineffective.

Due to the increasing social, political, and financial impact of cyber incidents,[1] it is imperative that South Africa's institutional design and legislative environment dealing with cybersecurity are working efficiently. To this end, we recommend

[1] See, for instance, Van Niekerk, B. (2017). An analysis of cyber incidents in South Africa. *The African Journal of Information and Communication* (AJIC), vol. 20: 113-132. Available at: https://doi.org/10.23962/10539/23573.

ICASA to facilitate a cyber maturity assessment of the country, in order to identify specific points of policy interventions that will inform an overall National Cybersecurity Strategy. The implementation of the National Cybersecurity Strategy should be underpinned by a comprehensive cybercapacity building programme, to develop competences, resilience, and trust in the Internet.

We would like also to confirm our availability for making oral representations should the Authority decide to hold public hearings.

For further information, Research ICT Africa can be contacted via:
info@researchictafrica.net or at +27 21 447 6332.

Acknowledgements

This submission was prepared by Dr Enrico Calandro, with valuable inputs, contributions and revisions by Anri Van Der Spuy and Dr Ian Brown. Any errors or omissions of course remain the author's own.

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

Introduction

A relatively recent innovation, the Internet is a 'network of networks'[2] which enables communication between networks on a global[3] and mostly public[4] scale – making it a particularly difficult governance challenge. It is more than the sum of its technological parts; a network of interactions and relationships which extends beyond technology and has the potential to enable human rights online and offline, to empower users and communities, and to facilitate sustainable development in line with the United Nations' *Agenda for Sustainable Development 2030*.[5]

But along with these opportunities for growth and development, the Internet also poses a number of risks which become increasingly visible and prevalent as it becomes more central to societies around the world (e.g. cybersecurity, hate speech, data breaches, misinformation, and online abuse). It also continues to evolve at a significant pace, continuously introducing new governance and regulatory challenges, with the growing importance of technologies like the Internet of Things (IoT) and Artificial Intelligence (AI).

These challenges apply globally, but are especially difficult to address in developing country contexts like South Africa. One key component of building a more inclusive and trustworthy Internet – one which can support sustainable development and economic growth rather than only expose South Africans to undue risks – is ensuring that the infrastructure underpinning the Internet itself is secure, safe and resilient. On the other hand, the Internet should be a space which protects private communications and the privacy of its users.

Growing cyber threats and cyberattacks pose a significant concern for the private and public sector in South Africa alike, and the country is not well enough

---

[2] Mathiason, J. (2009:7). *Internet Governance: The new frontier of global institutions*. Oxon: Routledge.

[6] Mueller, M., Mathiason, J. & Klein, H. (2007:244). The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance: A Review of Multilateralism and International Organizations*, 13(2): 237-254.

[4] MacLean, D. (2004:77). 'Herding Schrödinger's Cats: some conceptual tools for thinking about Internet Governance.' In MacLean, D. (Ed.) (2004), *Internet Governance: a Grand Collaboration*. New York: United Nations ICT Task Force Series 5, 73-99.

[5] UNGA. Resolution adopted by the General Assembly on 25 September 2015: Transforming our world: the 2030 Agenda for Sustainable Development (A/Res/70/1). (2015b, October 21). Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.

prepared to tackle an increasing number of reported incidents,[6] from data exposure to rising hacktivism[7] against targeted state-owned or political entities.[8] Existing weaknesses and flaws in the Internet's physical infrastructure and protocols[9] also require urgent mending and intervention by a multitude of stakeholders.[10]

This is particularly worrying as the Internet is also becoming a precondition for participation in today's society in many parts of the world. The Internet is an enabling infrastructure which is central to everything from the provision of e-government services to procuring benefits, performing work, accessing finance, or gaining further education. People who are not participating in (online) network societies[11] might therefore find it increasingly difficult to reap the benefits in (offline) societies if they remain unconnected.[12] Furthermore, many of the people who are yet to come online are also the poorest in society and therefore more

---

[9] Mitrovic, (2018) for instance, lists South Africa as one of the ten most vulnerable countries to cyberattacks globally. Mitrovic, Z. (2018). *Can BRICS boost cybersecurity of its member countries?* VM Advisory. Available at http://vmadvisory.com/cybercrime/

[7] Hacktivism refers to a form of openly political hacking. See, for instance, Wray, S. (2013). Electronic civil disobedience and the world wide web of hacktivism. Available at http://gloriagduran.com/wp-content/uploads/2013/03/netaktivizam.pdf. For an historical overview of the phenomenon, see McCormick., T. (2013). Hacktivism: A Short History. *Foreign Policy*. Available at https://foreignpolicy.com/2013/04/29/hacktivism-a-short-history/

[8] Van Niekerk, B. (2017). An analysis of cyber incidents in South Africa. *The African Journal of Information and Communication (AJIC),* vol. 20: 113-132. Available at: https://doi.org/10.23962/10539/23573.

[9] Network vulnerabilities include anything that poses a potential avenue for attack or security breach against a system. See Awodele, O., Onuiri, E., E., and Okolie, S. O. (2012). *Vulnerabilities in Network Infrastructures and Prevention/Containment Measures*. Proceedings of Informing Science & IT Education Conference (InSITE) 2012. Available at http://proceedings.informingscience.org/InSITE2012/InSITE12p053-067Awodele0012.pdf, for a comprehensive list of network vulnerabilities.

[10] In order to protect the public core of the internet infrastructure, a multistakeholder Global Commission on the Stability of Cyberspace was set up in February 2017 with the aim of "supporting policy and norms coherence related to the security and stability in and of cyberspace." See https://cyberstability.org/ for further information.

[11] Castells, M. (2005). The Network Society: From Knowledge to Policy (Chapter 1). In Castells, M. & Cardoso, G. (Eds.). (2005). *The Network Society: From Knowledge to Policy*. Washington DC: Center for Transatlantic Relations. Available at: www.umass.edu/digitalcenter/research/pdfs/JF_NetworkSociety.pdf.

[12] Elder, L., Samarajiva, R., Gillwald, A., & Galperin, H. (2013:73). in_focus - Information Lives of the Poor: Fighting poverty with technology. IDRC. ISBN: 9781552505717

vulnerable and susceptible to risk[13] as they often tend to lack the necessary digital literacy skills to know how to ameliorate risks when they do eventually gain Internet access.

In order for governments' institutions, the private sector, civil society organisations, and users to be equipped with the right tools and information to help them protect themselves against cyber threats, and to ensure that critical information infrastructures are resilient in the face of current and emerging challenges[14], we would like to recommend the following three foundational actions to ICASA to bolster South Africa's cyber readiness:

1) ICASA should **facilitate an empirical, independent, and impartial Cybersecurity Maturity Assessment (CMA)** in the country to identify the stage of maturity across a number of indicators related to cybersecurity: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training and skills; legal and regulatory frameworks; and standards, organisations, and technologies. Through the assessment it will be possible to identify specific points of policy intervention to effectively implement the National Cybersecurity Policy and the recently passed Cyber Crime Law.
2) **Contribute to the drafting of a National Cybersecurity Strategy (NCS)**, to review the vision, high-level objectives, principles and priorities that will guide South Africa in addressing cybersecurity; to clarify who are the stakeholders tasked with improving cybersecurity of the nation, what are their respective roles and responsibilities, and what are their modalities of collaboration. A NCS is also expected to include a description of the steps, programmes and initiatives that the country will undertake to protect its national critical infrastructure and, in the process, increase its security and resilience. The NCS should be implemented in a collaborative way between relevant government organs, the private sector, civil society organisations, and academia. Specific points of intervention, modalities of coordination between different organs of state, and between all stakeholders should emerge from the CMA and can help create an evidence-based NCS that can support the development of South Africa's digital economy.
3) Based on the findings from the CMA, ICASA should **support the implementation of a capacity building programme** for public officials, along with national cyber hygiene interventions and awareness campaigns

---

[13] Mansell, R. (1999). Information and Communication Technologies for Development: Assessing the potential and the risks. *Telecommunications Policy*, 23(1): 35-50.

[14] See OECD Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy (2008). *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*. [C(2008)35]. Available at http://www.oecd.org/sti/40825404.pdf

on how to be safe and secure online to improve information security practices and to inform Internet users on security requirements and appropriate online behaviour. ICASA should support both the Department of Telecommunications and Postal Services (DTPS) and the Department of Science and Technology (DST) to implement such initiatives.[15] The CMA will provide much-needed insight into: a) what skills and knowledge is available and missing in the country; and b) what economic and human resources are currently available (and what additional resources are needed) to deliver such programmes.

Setting the scene: National context on cybersecurity

Definitions

The 2012 National Cybersecurity Policy Framework (NCPF) has adopted the ITU definition of cybersecurity, according to which cybersecurity "is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets".[16] This all-inclusive definition refers to the need for adopting a multi-sectoral and multi-disciplinary approach to improve the resilience of information systems against attacks and accidental damage. Such an approach encompasses the strategic, legal, regulatory, as well as technological and non-technological mechanisms that need to be put in place with the aim of protecting different elements of the Internet infrastructure,[17] end-user devices, and other connected devices[18] (including the data and information stored or transmitted by them[19]).

---

[15] The National Cybersecurity Policy framework (NCPF) makes reference to capacity building in two ways: first, it mandates the DTPS to develop Cybersecurity Awareness platforms and program; second, it mandates the Department of Science and Technology (DST) with the responsibility for the "development, co-ordination and implementation of national capacity development programme". Nevertheless, very little has been done and achieved so far. See See also Biermann, E., and Van Der Waag-Cowling, N. (2018). Mind the Gap: Addressing South Africa's cybersecurity skills shortage. *Daily Maverick*, 13 July. Available at https://www.dailymaverick.co.za/article/2018-07-13-mind-the-gap-addressing-south-africas-cybersecurity-skills-shortage/.

[16] DTPS (2015:80). *National Integrated ICT Policy Review Report*. and ITU (2008). *SG17, ITU Lead Study Group on Telecommunications Security, Security Compendium Part 2 – Approved ITU-T Security Definition* (ITU: Geneva, September, 2008). Ref. 3.2.4/X.1205, p. 27.

[17] Including Internet eXchange Points (IXP), datacentres, cable operators, enterprise/institutional networks, academic network (NRENs), Content Delivery Networks (CDN), telecom operators (landline and mobile).

[18] For instance, smart watches, sensors, IoT devices, etc.

[19] Orji, U., J. (2012). *Cybersecurity Law and Regulation*. Wolf Legal Publishers (WLP): The Netherlands.

Although cybersecurity is primarily concerned with the protection of cyberspace and ICTs from all forms of cyber threats,[20] the definition of cybersecurity includes also issues beyond the protection of IT equipment, devices, and digital infrastructure, to include cyber harm beyond the online realm.

Cybersecurity means different things to different stakeholders. For instance, from a technological perspective, cybersecurity refers to technologies developed to safeguard computer systems and the information stored on such systems. From an organizational perspective, cybersecurity implies the technical and non-technical measures taken by an organisation to ensure the availability, confidentiality and integrity of its computers and information networks as well as the data stored or being communicated by them.

Certainly relevant for the work of ICASA, a more specialised definition of telecommunications security refers to the measures and controls taken to ensure the security of information being transmitted by telecommunications networks and the security of telecommunications networks and infrastructures. This implies the application of security measures to telecommunications systems, and regulatory interventions, in order to achieve objectives such as:

a) Denying unauthorised persons access to information of value;

b) Ensuring the authenticity of information handled by telecommunications systems;

c) Preventing the disruption of telecommunications services; and

d) Ensuring the resilience of telecommunications networks.[21]

The interrelation between telecommunications security and cybersecurity arises from the continued convergence of ICT and telecommunications technologies. Today, smartphones also perform the functions of a personal computer. In a converged digital environment, telecommunications networks connect all forms of electronic communication devices. They provide a linkage for computers, computer systems and electronic databases located all over the world, thus creating the global information infrastructure which is presently known as "the Internet". Thus, telecommunications networks create the necessary backbone for the exchange of communication between electronic communication devices which maybe either be computers or other telecommunication devices. As such, they need to be protected, ensuring network integrity and resilience, in order to build a more inclusive and trustworthy digital economy and society.

From a more technical point of view, cybersecurity refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The concept broadly extends to ensuring

---

[20] *Ibidem.*

[21] *Ibidem.*

the confidentiality, integrity, and availability of data.[22] Information integrity refers to the protection of information from being changed by unauthorized parties. It ensures that information in digital networks are protected against unauthorized modification, deletion, creation, relocation and destruction. Reliability also plays an important role in ensuring information security and network integrity. Reliability is an attribute of any computer-related component (software, or hardware, or a network, for example) that consistently performs according to its specifications.

In fulfilling its mandate of promoting the interests of consumers, ICASA is an implementing agency which should ensure not only information security and network integrity, but also reliability through setting technological standards which protect the availability, confidentiality and integrity of IT equipment and networks.

Context

The institutional design and legislative context of cybersecurity in South Africa is complex and fast evolving. It involves a number of entities that have not traditionally been involved with ICT issues or their governance.

In 2017, South Africa ranked 58th in the International Telecommunication Union (ITU)'s *Global Cybersecurity Index.*[23] In Africa, although South Africa is placed in the leading stage, which includes countries that have demonstrated a high commitment to cybersecurity, it only ranked 6th (preceded by Mauritius, Rwanda, Kenya, Nigeria, and Uganda).[24]

South Africa is signatory to international treaties such as the 2014 *AU Convention on Cyber Security and Personal Data Protection*[25] and the 2011 *Budapest Convention on Cybercrime*,[26] but has yet to ratify them. These treaties recognise that the Internet, being a global network, requires a legislative approach to cybersecurity which is harmonized with international approaches, and enables international cooperation in order to efficiently combat cybercrime.

Nationally, the foundational legislation in South Africa from which the other regulations related to cybersecurity derive is the 2002 *Electronic Communications*

---

[22] *Ibidem.*

[23] International Telecommunications Union (2017). *Global Cyber Index*. Geneva: ITU. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf,

[24] It also needs to be noted that GCI does measure cybersecurity in terms of cyber readiness or maturity, but only the legislative measures and policies on paper related to cybersecurity.

[25] Adopted on the 27 June 2014. Available at https://au.int/en/treaties/african-union-convention-cybersecurity-and-personal-data-protection

[26] CETS No.185. Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

and Transactions Act (ECTA).[27] The *Regulation of Interception of Communications and Provision of Communication-Related Information Act* (RICA) was also promulgated in 2002.[28] The *Protection of Personal Information* (POPI) Bill was released in 2009, and enacted in 2013,[29] but has only partially come into full effect.[30] The *National Cybersecurity Policy Framework* (NCPF) was released at the end of 2015,[31] followed by drafts of the *Cybercrimes and Cybersecurity Bill* [32]. The final version of the bill is a *Cybercrime Bill* and is in the process of being enacted.[33]

From an institutional design point of the view, South Africa has adopted an interagency approach to cybersecurity. The Government recognised that the issue of cybersecurity is cross-cutting and cannot be addressed by one department alone at an early stage.[34] In line with this, a number of Government departments are involved in cybersecurity. These include the *Cabinet Justice, Crime Prevention and Security Cluster* (JCPS Cluster); led by the *Minister of Justice*, which was in charge of reviewing all related legislation to ensure harmonisation and alignment. The *Department of Telecommunications & Postal Services* (DTPS) is part of the *Cyber Response Committee* (CRC) established under the Cluster and is thus integrally involved in ensuring alignment with the ECTA. The *State Security Agency* is tasked with the overall responsibility of cybersecurity and is working together with other relevant departments on this, including DTPS.

---

[27] Act No. 25 of 2002. Available at https://www.gov.za/documents/electronic-communications-and-transactions-act

[28] Act No. 70 of 2002. Available at https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13

[29] Act No. 4 of 2013. Available at https://www.gov.za/documents/protection-personal-information-act

[30] Michalsons (2018). POPI Act summary in plain language | Find answers. Available at https://www.michalsons.com/blog/popi-act-summary-in-plain-language/18618
According to the law firm Michalsons, it will probably commence in the first quarter of 2019.

[31] State Security Agency (2015). The National Cybersecurity Policy Framework. Available at https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000.

[32] B—2015. Available at http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf

[33] Michaelson (2018). *Cybercrime Bill in South Africa*. Available at: https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa. According to Ellipsis, "The Department of Justice and Constitutional Development presented a radically amended version of the Bill to the Portfolio Committee for Justice and Correctional Services on 23 October 2018. The biggest shift is the removal of provisions relating to cybersecurity, necessitating the renaming of the Bill from the "Cybercrimes and Cybersecurity Bill" to the "Cybercrimes Bill"". Available at: https://www.ellipsis.co.za/cybercrimes-and-cybersecurity-bill/.

[34] Department of Telecommunications & Postal Services (DTPS) (2014). National Integrated ICT Policy Discussion Paper. Options paper.

The *National Cyber Policy Framework* (NCPF) was published by Cabinet in 2012 to set out measures and mechanisms for coordination across government. It mandated the DTPS to establish a National Cybersecurity Hub[35] to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents.[36] The hub is tasked with enhancing interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society.[37]

Not only state organs have put in place processes and structures to deal with cybersecurity. A private-sector led initiative, iCode,[38] has for instance developed a new voluntary code of practice to improve cybersecurity for end users.[39] The initiative was developed by South Africa's Internet Service Providers' Association (ISPA) and aims at making it safer for South Africans to be online by encouraging Internet Service Providers (ISPs) to educate their customers while monitoring[40] their networks to identify customers whose machines are possibly infected with malware.

In terms of cybersecurity standards, .zaDNA, the *South African Domain Name Authority*, has already adopted the DNSSEC protocol, protecting the integrity of data about the South African domain names it oversees.[41]

While the adoption of a *National Cybersecurity Policy Framework* (NCPF) is a positive step towards coordinating efforts, the NCPF appears to be difficult to implement, and that is one of the reasons why is also being implemented rather slowly.[42] The various organisations and their links into yet more structures suggest that coordination between many rivalrous ministers will be problematic. Other

---

[35] The Cybersecurity Hub is one of the national Computer Security Incident Response Teams (CSIRTs) mandated by the country's National Cybersecurity Policy Framework (NCPF), under the Department of Telecommunications and Postal Services (DTPS). Others are the South African National Research Network (SANReN CSIRT), the ECS-CSIRT, which serves as the South African Government CSIRT, and private sector led CSIRT, such as the First National Bank CSIRT.

[36] State Security Agency, Republic of South Africa (2012). *National Cyber Security Framework for South Africa*. Government Gazette, 4 December 2015.

[37] https://www.cybersecurityhub.gov.za/ .

[38] See https://www.icode.org.za/about.php.

[39] ISPA (2011). *Press release: ISPA to Launch Cyber Security Code in South Africa*. Available at: https://ispa.org.za/press_releases/ispa-to-launch-cyber-security-code-in-south-africa/.

[40] Traffic monitoring is done in such a way that users' privacy is always protected.

[41] See ZACR DNSSEC Policy Practice Statement Framework. Available at https://www.registry.net.za/downloads/u/zacr-dps-signed.pdf.

[42] Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication (AJIC)*, vol. 20: 83-112.

issues about the effectiveness of its implementation are related to the adaptation of the policy document to the South African legal and political systems and cultures, and to the degree to which it has planned an institutional arrangement for which it does not have the administrative and technological skills to deliver.[43]

In addition, the current institutional arrangement for cybersecurity lacks mechanisms for information flow regarding cybersecurity in government departments[44] and has been criticised[45] for its potential limited transparency or oversight, considering that the Cybersecurity Response Committee, in charge of strategy and decision-making, is chaired by the Director-General of State Security.

Within this complicated institutional design, ICASA, structured by the *ICASA Act*[46] is expected to change if the *Draft Communications Act Amendment Bill* (2017) is passed in its current form. The *Draft Electronic Communication Act Amendment Bill* (2017) suggests to merge ICASA, The Universal Service and Access Agency of South Africa (USAASA), and the .za Domain Name Authority (.ZADNA) into a new 'Economic Regulator' under the newly merged Ministry of Communications and Department of Telecommunications & Postal Services.

In a submission made on January 2018[47], Research ICT Africa has expressed its concerns regarding the impact that the Amendment Bill will have on the powers, competencies, and independence of ICASA, considering that there is an undercurrent throughout the Bill that asserts the role of the Department of

---

[43] *Ibidem*. See also Biermann, E., and Van Der Waag-Cowling, N. (2018). Mind the Gap: Addressing South Africa's cybersecurity skills shortage. *Daily Maverick*, 13 July. Available at https://www.dailymaverick.co.za/article/2018-07-13-mind-the-gap-addressing-south-africas-cybersecurity-skills-shortage/. According to the authors, South Africa is failing to produce enough cybersecurity specialists to secure its digital space, cybersecurity expertise is rather limited and the Department of Science and Technology (DST), which is mandated by the NCPF to develop, coordinate, and implement national capacity development programme, has failed so far to do so.

[44] Patrick, H. (2015). *Security information flow in the public sector: KZN health and education*. PhD thesis. University of KwaZulu-Natal, Durban.

[45] Privacy International (2018). State of Privacy South Africa. Available at https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa#commssurveillance

[46] No. 13 of 2000. Available at https://www.icasa.org.za/independent-communications-authority-of-south-africa-act-2000

[47] Research ICT Africa (2018). written comments on the Electronic Communications Amendment Bill. Available at https://researchictafrica.net/wp/wp-content/uploads/2018/02/2018_Research-ICT-Africa-submission-to-South-Africa-parliament.pdf

Telecommunications & Postal Services (DTPS) and its Minister over that of ICASA, potentially downgrading the independence of the latter.[48]

Existing research on cyber readiness, cyber risks and cyber incidents

A number of public and private organisations alike have been monitoring and reporting on cybercrime and cyberincidents in South Africa.

In 2017, a cyber readiness report produced by DTPS[49] argued that the three top challenges facing organisations in South Africa with regard to cybersecurity were (a) insufficient skills (57%); (b) lack of in-house skills (49%); and (c) a lack of awareness on cyber risks (39%). This result indicates the importance of skills development and recruitment of specialised staff, together with the need for creating awareness. Targeted malicious emails (i.e. spam, phishing emails and attractive links) and ransomware were mentioned as threats of significant concern to organisations.

Considering that both targeted malicious emails and ransomware have become more widespread in recent years, the DTPS report recommended that "*more awareness is required to educate organisations about the dangers of attachments and safe surfing practices, to prevent their systems from being taken hostage"*[50]. On a positive note, of the organisations surveyed, almost half belonged to a Computer Security Incident Response Team (CSIRT) and 22% were obliged to report incidents.[51] Another government organ which conducts research on cybersecurity is the South African Government CSIRT, which is currently under the State Security Agency and produces a public daily ICT Information Security Report.[52]

An increasing number of Internet measurement platforms collect data on BGP hijack detection to produce security reports.[53] or deal with DDoS monitoring.[54] In addition, a few commercial reports on cybersecurity point to realities as

---

48 Calandro, E., Gillwald, A., Lewis, C., Mothobi, O., and Rademan, B. (2018). *Submission on the South African Electronic Communications Amendment Bill*. Available at: https://researchictafrica.net/2018/02/06/submission-on-eca/.

49 Although it is positive sign that the DTPS has embarked in a cyber readiness assessment, the research output only superficially analyses the cyber maturity level achieved in the country.

50 *Ibid*.

51 According to the DTPS, through CSIRTs, networking and sharing of incident information can help organisations to correct weaknesses. CSIRTs serve as a single point of contact for reporting incidents and they help to disseminate important incident-related information.

52 Reports are available at http://www.ssa.gov.za/CSIRT.aspx.

53 See, for instance, Oracle Dyn, available at https://dyn.com/web-application-security/.

54 See Thousandeyes, available at https://www.thousandeyes.com/solutions/ddos-monitoring.

experienced by citizens and firms but offer little specific information about South Africa. For instance, two of these popular reports are Akamai's *State of the Internet Security*[55] and Cisco's *Annual Cybersecurity Report*.[56]

Internet users' data on South Africa's cyberthreats is also available. The Symantec's *Internet Security Threat Report*[57], for instance, has set up a large collection network of civilian cyberthreats which represents a comprehensive collection of cybersecurity threat data. The network monitors threat activities for over 175 million endpoints located in 157 countries through a combination of proprietary technologies and measurement platforms. The report disaggregates the data at a country level and includes South Africa. Other organisations such as CyberGreen provide levels and trends of risk posed to others by the country, break downs the risk source by Autonomous System (AS),[58] and provide detailed country reports.

Research conducted by Van Niekerk (2017) on cyber incidents in South Africa documented a total of 54 incidents spanning 23 years, from April 1994 to the end of 2016. Most of the incidents had an impact on data exposure, in addition to advanced persistent threat (APTs) infections, including cyber espionage.

Van Niekerk also reported that South African mobile operators were severely affected by cyber incidents. In 2013, a flaw in Vodacom's portal reportedly allowed any subscriber to access high level account summary information linked to any phone number, and in 2014, a fault was similarly reported in Cell C's portal, enabling access to many customer records. In July 2009, a criminal group allegedly managed to acquire duplicate SIM cards that allowed for the interception of online banking one-time PIN codes (OTPs) for bank accounts which were compromised via phishing. The group reportedly managed to steal approximately ZAR7 million from the compromised accounts. In 2013, MTN and affiliated service providers suffered a service outage due to a DDoS attack. Again, in 2015, MTN experienced performance degradation due to a second DDoS attack.

---

[55] The report covers "botnet", from web crawlers to site scrapers to account takeover tools or even DDoS tools. Available at: https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp.

[56] Report available at http://www.cisco.com/c/en/us/products/security/security-reports.html.

[57] Report available at https://www.symantec.com/security-center/threat-report

[58] CyberGreen reports a measure of DDoS risk to others by country, by Autonomous System (AS), and by such alternate entities (e.g., enterprises) as seem relevant. That crude measure is the count of nodes within the scope of control of the country, the AS, or the entity otherwise defined that have the configuration that allows them to participate in a DDoS. The count will be reported by protocol and in sum across all four protocols. Countries, ASs, and alternate entities will be ranked by the count of nodes available to the operator of a DDoS amplification attack, i.e. a rank of 1 is that of the highest risk. It is that rank that is the v2.0 CyberGreen Index value. See https://stats.cybergreen.net/country/south-africa/ for data on South Africa.

A nationally-representative ICT access and use survey conducted in 2017 by Research ICT Africa[59] found that 6.81% of Internet users in the country have been conned over the Internet and lost money. With reference to account hacking, the surveys found that less than 10% of Internet users have experienced such a problem.

Although freedom of expression can at times have negative consequences, especially if the opinion that is expressed causes damage or trauma to somebody else, in order to avoid such consequences, constitutional limitations are in place in relation to what can be freely expressed and what is instead forbidden due to its potential to cause harm. Nevertheless, on social media, users may have used these platforms to harm others, not only with the intention of doing so, but also due to a lack of awareness, limited media literacy, or even a perception of freedom that goes beyond constitutional limits. In relation to cyber bullying, which is criminalised under the current *Cybercrime Bill*, the surveys found that only 3.93% South African Internet users seem to have ever experienced cyber bullying.[60]

Recommendations: navigating cyber complexity through a coordinated National Cybersecurity Strategy

1) From research and development to cyber maturity assessments

Research on cybersecurity, although scattered across different private, not-for-profit, public and academic organisations, is increasingly being conducted; and a growing number of existing and new organisations are monitoring cyber threats and cyber incidents in South Africa.

Considering the complexity of measuring threats, risks, and harms in cyber contexts, as well as the current lack of skills in the regulator to deal with these issues, we recommend that ICASA should rather adopt the role of facilitating the collection and analysis of these indicators. For instance, the regulator could request ISPs and other Electronic Service Providers to report on cyber threats to national CSIRTs that are already collecting and analysing different types of indicators. In the current institutional design for cybersecurity, the National Cybersecurity Hub is the central point for the collection of data on cybersecurity incidents, and is tasked with enhancing interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society.

Taking into account the complex institutional arrangements currently underpinning an advanced cybersecurity policy and legal framework in the country, we recommend that a cyber maturity assessment (CMA) be undertaken to

[59] See www.afteraccess.net.

[60] It needs to be noted that the survey does not sample children, and they are notoriously the most affected by cyber bullying.

obtain an empirical, independent, and impartial evaluation of the cyber maturity level of the country. This would enable ICASA to effectively implement a comprehensive methodology for the review of South Africa's cybersecurity capacity and to then inform resource allocation for cybersecurity capacity investment.

One such established CMA is that one developed by the Global Cybersecurity Capacity Centre (GCSCC) at the University of Oxford. In a comprehensive framework which assesses the level of capabilities which are foundational to building resilience of a country, the assessment evaluates cyber maturity over five different dimensions: 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.

2) (Lessons for) developing a National Cybersecurity Strategy

With regards to private sector cooperation and industry regulation, some lessons on cybersecurity regulation can be learnt from two examples in African countries.

In Mauritius, according to the country's *National Cyber Security Strategy*, regulatory bodies should establish, control, inspect and enforce regulations with regard to cybersecurity, and encourage organisations to adopt security best practices and guidelines. Mauritius' national cybersecurity strategy is implemented through a collaborative arrangement which not only extends to public and private sector entities, but also to stakeholders from different sectors (including the technical community, the banking and finance sectors, business process outsourcing, health, tourism, and energy sectors). The regulator Information and Communication Technologies Authority (ICTA) is considered as one of the main stakeholders across all projects of the Action Plan of the National Cybersecurity Strategy, and it is involved in a number of projects dealing with securing cyberspace and with establishing a front line of defence against cyber crime. The regulator is also involved in the development and implementation of a Critical Information Infrastructure Protection (CIIP) framework, and in the development and implementation of a cyber crisis management plan.[61]

In Ghana, a *National Cybersecurity Policy and Strategy* (NCSPS)[62] has been developed and the strategy deals with many aspects related to cybersecurity, including capacity building, cybercrime legislation, standardisation and safeguards. Within this context, the National Communications Authority (NCA) has

---

[61] Van Der Spuy, A., Calandro, E., and Brown, I. (2018). Collaborative cybersecurity: the Mauritius case. *Policy Brief 1: Africa Digital Policy,* October 2018. Available at https://researchictafrica.net/wp/wp-content/uploads/2018/11/Policy-Brief-ADPP-N-1-Collaborative-Cybersecurity-Mauritius-Case.pdf.

[62] Ministry of Communications, Republic of Ghana (2014). Ghana National Cyber Security Policy & Strategy. Available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Ghana_Cyber-Security-Policy-Strategy_Final_0.pdf

been very active in providing training on cybercrime and electronic evidence for judges and prosecutors, in collaboration with the Council of Europe under the Global Action on Cybercrime Extended (GLACY+) project.[63]

The NCA has also established a CERT which forms part of the investigative branch of NCA. It provides proactive cybersecurity services such as advisories, security monitoring services and cybersecurity incident management to protect the NCA and its licensees or entities in the telecommunications sector. The primary mission of the NCA-CERT is to provide incident handling services for its internal constituents, the NCA, and to facilitate incident coordination, information exchange and analysis to look for trends and patterns in incident activity for its external constituents, licensed Network Operators and their subscribers.[64] The NCA-CERT deals with incident reporting, incident handling, and has an emergency contact.

National Cybersecurity Strategies can take many forms and can go into varying levels of detail, depending on the country's objectives and levels of cyber readiness. As in the case of Mauritius and Ghana, a South African cybersecurity strategy would help to set out a vision, objectives, and priorities. A strategy would enable the government to look at cybersecurity holistically across the national digital ecosystem, instead of at a particular sector, objective, or in response to a specific risk. Based on the proposed maturity assessment, priorities can be set based on empirical research results, allowing South Africa to address real problems and therefore to promote trust in the online environment, in addition to improve cybersecurity awareness of the general public; or a combination of these issues.

Roles and responsibilities of ICASA would emerge from the maturity assessment and would be clearly defined and stated in the NCS. Not only roles and responsibilities will be identified based on an empirical assessment, but also the role of the regulator in the implementation of the strategy will be better defined.

A number of resources are available for the development of a NCS. For instance, the Global Forum on Cyber Expertise[65] has been mapping needs and resources in terms of national cyber strategy development and acts as a clearing house between countries requesting support, the donor community, and specialised

---

[63] See National Communications Authority (NCA) (2017). *Ministers for Communication and National Security Pledge to Support Efforts in Fight against Cybercrime*. Press Release. Available at: https://nca.org.gh/media-and-news/news/ministers-for-communication-and-national-security-pledge-to-support-efforts-in-fight-against-cybercrime/.

[64] See NCA CERT Charger & Mission, available at https://nca-cert.org.gh/index.php/about/charter-mission/.

[65] https://www.thegfce.com/.

academic or private research organisations and consultants who may help to efficiently support the development of the process.

3) Cyber capacity

A significant challenge where cyber capacity building is concerned is designing the process in such a way that it can be both effective and sustained over time. To achieve this objective, it is crucial to reflect on how different stages of cyber capacity building relate to specific development objectives, and how the distribution of responsibilities between individuals, governments, the private sector, civil society organisations, and the international community can influence the process in both positive and negative ways.[66] At the same time, given the speed with which technological progress is occurring, it is important to think of capacity building as a dynamic process whereby the needs of concerned stakeholders are in constant evolution.[67]

Capacity building projects aimed at law enforcement and judicial training, cyber crime or high-tech crime units, computer forensic capabilities, and IT security specialists require the commitment of substantial financial and human resources. But considering that the responsibility for cybersecurity is distributed among many stakeholders, cyber capacity building should extend beyond public officials.

Bringing together different stakeholders (such as public organisations, the private sector, CSOs, and users) to address cybersecurity challenges is not an easy task given the complexities of such collective endeavours.[68] The first step in overcoming those obstacles is for stakeholders to gain a better understanding of their specific roles and of the framework within which cyber capacity can be implemented. A working paper by Research ICT Africa has discussed the

---

[66] According to Pawlak, P. (2014). Developing capacities in cyberspace. *European Union Institute for Security Studies*. Available at https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_21_Cyber.pdf, the specific objectives of a cyber capacity building exercise are: 1) Prevention; 2) Protection; 3) Pursuit; and 4) Response.

[67] Calandro, E., and Pawlak, P. (2014). Capacity Building as a means to counter 'cyber poverty'. European Institute for Security Studies. Available at https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_21_Cyber.pdf.

[68] The government of Mauritius, for instance, in developing its national cybersecurity collaboration framework, it moved from a more hierarchical, prescriptive public-private partnership model to a more open and horizontal public-private initiative model based on a collaborative 'interplay' which included a wider range of stakeholders. The broader, less rigid 'interplay' model included users as targets of public awareness campaigns from law enforcement agencies and the national Computer Emergency Response Team (CERT). See Van Der Spuy, A., Calandro, E., and Brown, I. (2018). Collaborative cybersecurity: the Mauritius case. *Policy Brief 1: Africa Digital Policy,* October 2018. Available at https://researchictafrica.net/wp/wp-content/uploads/2018/11/Policy-Brief-ADPP-N-1-Collaborative-Cybersecurity-Mauritius-Case.pdf.

difficulties of such collaboration at length[69]. When built on mutual trust and developed around a clear strategy that limits abuse and sets realistic goals, collaboration in cybersecurity offers many benefits. Nevertheless, private parties are compelled to sometimes adopt state-like roles in becoming patrons of the public good to address cyber risks although they lack public awareness, scrutiny and/or democratic deliberation when they act as arbiters of the national interest. In addition, some may question the legitimacy of important state responsibilities (i.e. national security) being outsourced to private sector stakeholders with business imperatives, or the appropriateness of national or government resources being used to protect private critical infrastructure and private critical information infrastructure through publicly-sponsored capacity building programmes[70]. Therefore, there is a need to better understand collaboration in capacity building, how it should be organised and how it works in terms of funding and resource allocation.

Considering that cyber capacity is a costly, complex and time-consuming exercise, it is important to conduct maturity assessments in order to identify precise points of capacity interventions, and to allocate the few available resources where they are most needed.

Conclusions

Although the responsibility for cybersecurity is distributed among many stakeholders,[71] the state still plays an important role in creating a legal and policy environment that helps to protect the benefits of a safe, secure, and trustworthy Internet. In South Africa, law-making, law enforcement, defence, and sector regulation are the exclusive prerogatives of the state. Nevertheless, considering the difficulties and inefficiencies for the regulator associated with addressing information security and network integrity only through more traditional *ex-ante* regulatory action, ICASA could play an invaluable role in providing incentives for other stakeholders to report on cyber threats and cyber incidents, to embark on capacity-building activities, and to therefore implement the technical, human and financial resources needed to maintain safe and secure infrastructure and other IT equipment.

Challenges to the development of a safe, secure, and trusted cyber environment can be partly addressed with capacity building initiatives that improve resilience.

---

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

[70] *Ibidem*.

[71] See, for instance, a policy brief on collaborative models for cybersecurity. Van Der Spuy, A., Calandro, E., and Brown, I. (2018). Collaborative cybersecurity: the Mauritius case. Policy Brief 1: Africa Digital Policy, October 2018. Available at https://researchictafrica.net/wp/wp-content/uploads/2018/11/Policy-Brief-ADPP-N-1-Collaborative-Cybersecurity-Mauritius-Case.pdf.

This can be achieved by establishing and developing the right institutions, structures and norms, and enabling them to work in a coordinated way as defined by a National Cybersecurity Strategy. But this approach must be tailored to the situation on the ground, taking into account the level of cyber maturity achieved in South Africa.

Although the South African government has demonstrated increasing awareness of cybersecurity issues, existing capability to deter cybercrime and monitor or pursue cybersecurity seem insufficient and ineffective. The situation is further complicated by the fact that technical capacities and resources are generally limited at a regulatory level. Also, cybersecurity concerns in response to the widespread diffusion of mobile connectivity have often been addressed in isolation from the privacy and surveillance implications in South Africa, and at the moment this aspect seems largely overlooked.[72]

The predominantly security-based approach adopted by the Government risks becoming unsustainable and costly – hence undermining the benefits for society and the economy – if the overall approach to cybersecurity does not address structural risks (e.g. no clear allocation of resources, no clear inter-departmental and multistakeholder coordination) or if proper institutional design assessments are not put in place. Another example is the protection of critical infrastructure, where in order to improve the security of the most important infrastructural services (i.e. telecommunications, energy, water, transportation, the supply chain) there is a clear need to include elements that will enhance cyber resilience (i.e. CSIRTs, research, points of contact) in a broader framework that also includes multistakeholder collaboration, legal and personnel aspects.

Mainstreaming various procedural and cyber-specific 'add-ons' into existing policies and structures may result in the development of policies that are more resilient to all types of risks. Therefore, it might be more accurate to address challenges in cyberspace from a risk management perspective with its diverse policy responses, including technological adaptations, legislative frameworks, and collaborative institutional arrangements, and to address them through capacity-building activities properly designed through a National Cybersecurity Strategy underpinned by a cyber maturity assessment. In this scenario, the role and responsibility of the regulator is to facilitate this process, in order to ensure that critical information infrastructures are resilient in the face of current and emerging challenges.

---

[72] For instance, one of the key aspects of the South African emerging mobile-centric surveillance society is the SIM registration requirements.