DISCUSSION DOCUMENT

INQUIRY INTO THE ROLE AND RESPONSIBILITIES OF THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA IN CYBERSECURITY

Contents

1 EXECUTIVE SUMMARY 2

2 INTRODUCTION 5

3 METHODOLOGY AND LIMITATIONS 7

4 DEFINING CYBERSECURITY 7

5 THE SOUTH AFRICAN LEGISLATION 9

6 SOUTH AFRICAN GOVERNMENT CYBERSECURITY STRATEGY 16

7 INTERNATIONAL BENCHMARKING 23

8 PROPOSED CYBERSECURITY APPROACH FOR THE AUTHORITY..........................41

9 CONCLUSION...47

1. EXECUTIVE SUMMARY

1.1 This Discussion Document is the start of an inquiry in terms of section 4B of the Independent Communications Authority of South Africa, 2000 (Act No. 13 of 2000) ("**ICASA Act**") read with sections 2(n) and (q) of the Electronic Communications Act, 2005 (Act No. 36 of 2005) ("**ECA**") into the role and responsibilities of the Independent Communications Authority of South Africa ("**the Authority**" or "**ICASA**") in Cybersecurity. In order to fulfil its mandate of promoting the interests of consumers with regard to price, quality and the variety of electronic communications services and ensuring information security and network reliability, the Authority decided to solicit views and obtain information that will assist it to define its role in the Cybersecurity environment.

1.2 The rapid adoption in developing countries of new information and communication technology ("**ICT**") infrastructures such as the Internet is creating opportunities for these countries and its citizens to participate in the international flow of information, ideas, and commerce.[1] "More than 2 billion users send more than 88 quadrillion emails annually, and they register a new domain name with Internet Corporation for Assigning Names and Numbers every second of every day".[2]

1.3 It should be noted that while the Internet comes with many advantages, it has also introduced a new challenge to South Africa's national security. During the initial emergence of the Internet, safeguarding its security was less of a concern, but in recent years, the Internet has undergone exponential growth and protecting security of consumers, businesses and the Internet infrastructure is key.,

[1] Madon, S. (2000). The Internet and Socio-economic development: Exploring the interaction. Information, Technology and People. 13(2), 85–101.

[2] Rosenzweig, P 2013, Cyber Warfare: How conflicts in Cyberspace are challenging America and changing the world, e-book, accessed 19 September 2018, p.201 < https://books.google.co.za/books?id=-xNb99V6WWkC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>.

1.4 As cyber threats grow, security policy, technology and procedures need to evolve even faster to stay ahead of the threats. However, in reality, it has been observed that cybersecurity standards often lag the state-of-the-art and generally lag, to some degree, the state-of-the-practice. Advanced threats evolve and innovate on a daily basis whereas the Cybersecurity framework takes months, if not years, to gain consensus and to finally be implemented into law. Studies show that cybersecurity concerns cannot be resolved solely by market forces or by regulation but require a novel mix of solutions.[3]

1.5 This Discussion Document examines the role of various ICT regulators in the governance of cybersecurity in their respective countries. The aim is to benchmark or compare the role of the respective ICT regulators to the Authority's role and to consult on whether it is necessary for the Authority to adopt similar roles taking into account the confines of South African law.

1.6 The benchmark has revealed that cyber concerns are present in all countries, however each country combats the presence of cyber threats differently, and generally cybersecurity is not regulated by a single government institution but often government institutions work together, and assign work amongst themselves as follows:

[3] Anderson, R. (2001). Why Information Security is Hard–An Economic Perspective. Retrieved October 18,2007, from http://www.acsac.org/2001/papers/110.pdf

1.6.1 The technical aspect of cybersecurity is often handled by regulators.

1.6.2 the aspect of public awareness about risks associated with online life, e.g. loss of privacy, exposure of children to child abuse material, is left to regulators to conduct.

1.6.3 The cybercrime is regulated by the security clusters or government departments responsible for public safety in those jurisdictions.

1.7 It is recommended that, like many countries listed in this research, the Authority should consider adopting the following roles and responsibilities:

1.7.1 Private sector cooperation and industry regulation;

1.7.2 Capacity building;

1.7.3 Research and development; and

1.7.4 Regulation of Cybersecurity standards.

1.8 The Authority will consult with all interested parties before making a final determination on issues raised in this Discussion Document. Thereafter, the Authority will communicate its findings and positions through a Findings Document.

2. INTRODUCTION

2.1. The Authority is enjoined by the ICASA Act and the ECA to promote the interest of consumers with regard to the price, quality and variety of electronic communications services and to ensure information security and network reliability.

2.2. ICTs have become an indispensable part of our daily life. Today, these technologies support national security, ensure economic stability and enable social interaction within countries.

2.3. Interconnected networks have encouraged investment and facilitated new consumption models that have driven global economic growth. Information technology has become a key driver behind economic growth.[4] A panel study with 25 Organization for Economic Co-operation and Development (OECD) countries covering the period 1996–2007 was carried out to estimate various broadband impacts and reported that for every 10% increase in fixed broadband penetration, the GDP will increase by 1.38 in developing countries%[5]

2.4. The benefits brought about by these technologies intrinsically originates with vulnerabilities and the risk of exploitation. Cybercrimes such as phishing, spam, computer-related fraud and other similar offences are rapidly increasing and evolving in step with the development and adoption of new ICT services.[6] Cybersecurity is a growing global challenge.

2.5. The evolution of technology has resulted in access to the cyberspace, no longer being through a single medium, that is, the personal computer. Telecommunication devices and networks previously operated for voice access only have now evolved to comprise access to all Internet services. The evolution is not taking place in an unregulated environment however, telecommunication regulators have been existing to regulate the technical, economic and social uses of these services. In this respect, the technology evolution in the telecommunication sector imposes a need for evolution on the role of the regulators.

[4] Suffolk, J. 21st century technology and security – a difficult marriage.

2.6. Cybersecurity ensures that the public continues to enjoy the benefits that ICTs bring by managing the vulnerabilities and the risk of exploitation. Government, regulators, private sector organisations and individual users all have a responsibility to make efforts in creating a safe cyberspace.

2.7. The aim of this Discussion Document is to explore the evolving role of ICT regulators in the governance of cybersecurity in different countries, with the aim of deciding whether the Authority should adopt similar roles taking into account the confines of South African law.

Question 1: Does the evolution of technologies necessitate the regulatory function evolution of the Authority? Elaborate.

[5] http://pubdocs.worldbank.org/en/391452529895999/WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf

[6] Draft Background Paper on Cybersecurity: The Role and Responsibilities of an Effective Regulator ("**The draft background paper**"). The draft background paper was commissioned by the ITU Telecommunication Development Sector's ICT Applications and Cybersecurity Division and Regulatory and Market Environment Division. The draft background paper was prepared by Eric Lie, Rory Macmillan and Richard Keck of Macmillan Keck (Attorneys and Solicitors), for the 9th ITU Global Symposium for Regulators held in Beirut, Lebanon (10-12 November 2009). Available on http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

3. METHODOLOGY AND LIMITATIONS

This Discussion Document has been compiled using information gathered through a desktop research. The Discussion Document provides an explanatory and contextual discussion to issues. Where necessary it formulates the Authority's initial view and then poses questions to solicit responses that will enable the Authority to make a finding or establish a final view on matters. This will be done through a Findings Document. The Authority expects stakeholders to respond productively to the Discussion Document during the public consultation process.

4. DEFINING CYBERSECURITY

4.1. As a starting point it is important to reach consensus on the meaning of the term "cybersecurity". The term "cybersecurity" has emerged as a widely-used term, and although this may not be an issue when it is used in an informal setting, it can potentially cause considerable problems in the context of regulation of roles.

4.2. The online version of the Oxford English Dictionary defines cybersecurity as "the state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this".[7]

4.3. Further, the International Telecommunications Union Recommendation ITU-T X.1205provides a more extensive definition:

> "*Cybersecurity is the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, users, applications, services, telecommunications systems, and the totality of transmitted and/or*

[7] https://en.oxforddictionaries.com/definition/cybersecurity.

> *stored information in the cyber environment. Cybersecurity ensures the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. The security properties include one or more of the following: availability; integrity (which may include authenticity and non-repudiation) and confidentiality*".[8]

In the African context the African Union (AU) does not provide a definition for Cyber Security, however subscribes to the ITU definition. The AU states that Cybersecurity has many dimensions and people ultimately expect cyberspace systems to function in a trustworthy environment despite many potential threats. Different ways of thinking about cybersecurity entails liability laws coupled with new directions in education, training and operational practice [9]

4.4. in the Authority's view, when defining the term "cybersecurity", one must consider and include the following four aspects of cybersecurity:[10]

4.4.1. the Information Technology security perspective,

4.4.2. legal or law enforcement perspective,

4.4.3. national security perspective, and

4.4.4. economic perspective.

Question 2: How would you define cybersecurity?

[8] ITU-T Recommendation X.1205, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[9] Cybersecurity, http://pages.au.int/infosoc/cybersecurity https://au.int/en/ie

[10] International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

5. THE SOUTH AFRICAN LEGISLATION

5.1. In South Africa, cybersecurity has been identified as a critical component affecting National Security. More geographical regions of South Africa are becoming integrated into the global village, necessitating additional government initiatives aimed at bridging the digital divide and addressing cybersecurity. One of these initiatives is the development and implementation of a South African specific cybersecurity policy.

5.2. In the ensuing paragraphs, we provide a brief summary of the South African legal and regulatory framework governing issues affecting cybersecurity.

5.3. THE CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA, 1996 (ACT NO.108 OF 1996) ("THE CONSTITUTION")

5.3.1. South Africa is a constitutional democracy which means that the Constitution is the supreme law of the Republic, and its values must guide South Africa and its people. The following values and rights enshrined in the Constitution have a bearing on cybersecurity:[11]

5.3.1.1. the right to privacy in section 14(d), which includes the right not to have the privacy of their communications infringed;

5.3.1.2. Section 16 provides that everyone has the right to freedom of expression. This right in section 16 includes freedom to receive or impart information or ideas without interference by public authorities and regardless of frontiers; and

5.3.1.3. the right to access of information in Section 32, includes access to any information that is held by another person and that is required for the exercise or protection of any rights in the Bill of Rights.

[11] Papadopoulus, S & Snail, S. (2012). The law of the internet in South Africa.

5.4. THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) (“POPI”)

5.4.1. The purpose of POPI is, amongst others, to –

5.4.1.1. give effect to the constitutional right to privacy, by safeguarding personal information when processed by any person, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information and protecting important interests, including the free flow of information within the Republic and across international borders; and

5.4.1.2. regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.

5.4.2. Sections 19 to 22 of POPI sets out the basic security safeguards required for the reasonable protection of personal information.

5.5. THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002 (ACT NO. 25 OF 2002) ("THE ECTA")

5.5.1. The ECTA is a key legislation to ensure secure information security, it was promulgated to facilitate and regulate electronic communications and transactions, and it establishes a formal structure to define, develop, regulate and govern online or electronic-commerce (e-commerce) in South Africa. Critical for cybersecurity the ECTA provides for, inter alia, the following: Regulations of Public Key Infrastructure and authentication and accreditation for electronic signatures;

5.5.1.1. Legal, technical and operational framework for e-signatures usage;

5.5.1.2. Categories of electronic signatures;

5.5.1.3. Preferred Authentication Service provider for government, namely the South African Post Office Trust Centre;

5.5.1.4. Establishment of the South African Accreditations Authority; and

5.5.1.5. Appointment of cyber inspectors.

5.6. THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000 (ACT NO. 2 OF 2000) ("PAIA")

5.6.1. The PAIA was enacted to reaffirm citizens' rights of access to information enshrined in section 32 of the Constitution, subject to justifiable limitations. PAIA ensures and fosters a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information.

5.7. THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002 (ACT NO. 70 OF 2002) ("RICA")

5.7.1. The primary purpose of RICA is to assist law enforcement officials in obtaining information required to combat crime, by regulating the interception of certain communications, monitoring of certain signals and radio frequency spectrum and the provision of certain communications-related information.

5.8. THE ELECTRONIC COMMUNICATIONS ACT (ECA)

5.8.1. The ECA seeks to establish a regulatory framework, in line with technological and economic developments, to promote convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors.[12]

5.8.2. The Authority is enjoined by the ECA to:

5.8.2.1. promote the interests of consumers with regard to the price, quality and the variety of the electronic communications services (section 2(n));

5.8.2.2. ensure information security and network reliability (section 2(q));

5.8.2.3. prescribe standards for the performance and operation of any equipment or electronic communication facility, including radio apparatus (section 36 (1)) and

5.8.2.4. set standards aimed at protecting the integrity of the electronic communications network (section 36 (2)).

[12] Preamble to the ECA

5.9. THE ICASA ACT

5.9.1. Section 2 of the ICASA Act established the converged and independent regulator and sets out the manner in which ICASA is to exercise its powers and functions in terms of the underlying electronic communications and broadcasting legislations.

5.10. THE DRAFT CYBERCRIMES AND CYBERSECURITY BILL

5.10.1. In August 2015, the Department of Justice and Correctional Services ("**DCS**") published a draft Cybercrimes and Cybersecurity Bill ("the draft Bill"), to engage with interested parties and afford them an opportunity to make written representations. The purpose of the draft Bill is to make the internet a much safer space for South Africans. The draft Bill aims to deal with various aspects relating to cybercrime and cybersecurity and to that extent the Bill:

5.10.1.1. Creates offences and prescribes penalties; and

5.10.1.2. Imposes obligations on electronic communications service providers regarding aspects which may impact on cybersecurity.

5.10.1.3. Taking into account the public submissions received, in March 2017 the DCS published a revised draft of the Cybercrimes and Cybersecurity Bill in Government Gazette No. ("**the Bill**"), written submissions on the Bill were initially due by no later than 28 July 2017 however, the deadline for submissions was extended to 10 August 2017. The bill is currently under consideration by the National Assembly.

5.10.1.4. The Memorandum on the objects of the Cybercrimes and Cybersecurity Bill, 2007 ("**The Memorandum**") states that the primary aim of the Bill is to deal with cybercrimes and cybersecurity. The Memorandum further recognises that there is no general universally recognized definition of cybersecurity and proposes that the term "cybersecurity" can more readily be defined as "technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or a computer systems against cybercrime, damage or interference.

5.10.2. Should the Bill be enacted in its current form, electronic communications service providers will have new obligations placed on them to assist law enforcement with the investigation of cybercrimes. In this regard, the Bill also requires significant alignment with the RICA and POPI.

5.11. At an international level, South Africa has supported a series of resolutions of the United Nations ("**UN**") General Assembly (2010) concerning Computer Security Incident Response Teams ("**CSIRTs**"), protection of critical national infrastructure ("**CNIs**") and, more generally, the work of the UN Office on Drugs and Crime (UNODC, 2017).[13]

5.12. South Africa is a signatory to international treaties such as the Budapest Convention on Cybercrime (Council of Europe, 2001), but never ratified it. The Budapest Convention is the only international agreement that addresses cybercrime and is aimed at harmonising national laws and establishing international cooperation against cybercrime.

5.13. Further, South Africa has also signed, but not ratified, the African Union ("**AU**") Convention on Cyber Security and Personal Data Protection (AU, 2014). The draft AU Convention on cybersecurity sets out options for an AU-wide cybersecurity policy, lays the foundation for cyber ethics and regulates issues related to the use of electronic transactions, electronic signatures as well as an as institutional framework for the protection of personal data.

5.14. At a regional level, South Africa is a member of Southern Africa Development Community ("**SADC**"), and a number of guidelines and model laws have been developed as a way to promote common approaches to common problems. There is a SADC Model Law on Data Protection and the SADC Model Law on Cybercrime. With this guidance, each SADC country enacts its own laws and publishes its own related regulations, enabling the effective regulation of mobile financial services as a key component of the digital economy in the region.[14]

Question 3: Are there any other laws that the Authority should consider in determining its role with regard to Cybersecurity?

Question 4.: Section 2(q) of the ECA provides that one of the objects of the ECA is to "ensure information security and network reliability".

4.1 What is information security and network integrity and what is your understanding of the Authority's mandate in this regard?

4.2 Is the mandate to ensure network integrity and information security currently being fulfilled by the Authority?

Question 5: Section 36 (2) of the ECA provides that "standard[s] must be aimed at protecting the integrity of the electronic communications network", kindly provide your understanding of this section.

[13] http://wiredspace.wits.ac.za/bitstream/handle/10539/23580/AJIC-Issue-20-2017-Full-Issue-Print-on-Demand.pdf?sequence=3.

[14] http://wiredspace.wits.ac.za/bitstream/handle/10539/23580/AJIC-Issue-20-2017-Full-Issue-Print-on-Demand.pdf?sequence=3.

6. SOUTH AFRICAN GOVERNMENT CYBERSECURITY STRATEGY

6.1. The South African Government has implemented a number of strategic and tactical interventions including the National Cybersecurity Policy Framework ("**NCPF**") published on 4 December 2015. The NCPF recognises that the State is charged with implementing a Government led, coherent and integrated Cybersecurity approach which, amongst others, will:

6.1.1. promote a cybersecurity culture and demand compliance with minimum security standards;

6.1.2. Strengthen intelligence collection, investigations, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber warfare, cyber terrorism and other cyber ills;

6.1.3. Establish public –private partnerships for national and international action plans;

6.1.4. Ensure the protection of National Critical Information Infrastructure (NCII); and

6.1.5. Promote and ensure a comprehensive legal framework governing cyberspace.

6.2. The key aims of the NCPF are to:

6.2.1. Centralise coordination of cybersecurity activities, by facilitating the establishment of relevant structures, policy frameworks and strategies in support of Cybersecurity in order to combat cybercrime, address national security imperatives and to enhance the information society and knowledge based economy;

6.2.2. Foster cooperation and coordination between Government, the private sector and civil society by stimulating and fostering a strong interplay between policy, legislation, societal acceptance and technology;

6.2.3. Promote international cooperation;

6.2.4. Develop requisite skills, research and development capacity;

6.2.5. Promote a culture of Cybersecurity; and

6.2.6. Promote compliance with appropriate technical and operational Cybersecurity standards.

6.3. The NCPF implementation is supported by the following institutions:

6.3.1. The Cybersecurity Response Committee

6.3.2. Cybersecurity Centre

6.3.3. Cybersecurity Hub

6.3.4. National Computer Security Incidence Response Team (NCSIRT) and sector CSIRT

6.3.5. National Verification of Information Security Products and Systems

6.3.6. Protection of the NCII.

6.4. The objective of the framework is to balance the risks associated with the use of information systems and the indispensability of extensive and free use of information technology to the functioning of open and modern society.

6.5. In implementing the NCPF, the Minister of Telecommunications and Postal Services unveiled the National ICT Forum ("**the Forum**"). The main objective of the Forum is to bring together government, labour, civil society and business to discuss critical sector issues that can facilitate the acceleration of socio-economic development. Therefore, the Forum is a platform for engagement around how best to use technology to modernise society.

6.6. The forum is made up of four chambers:

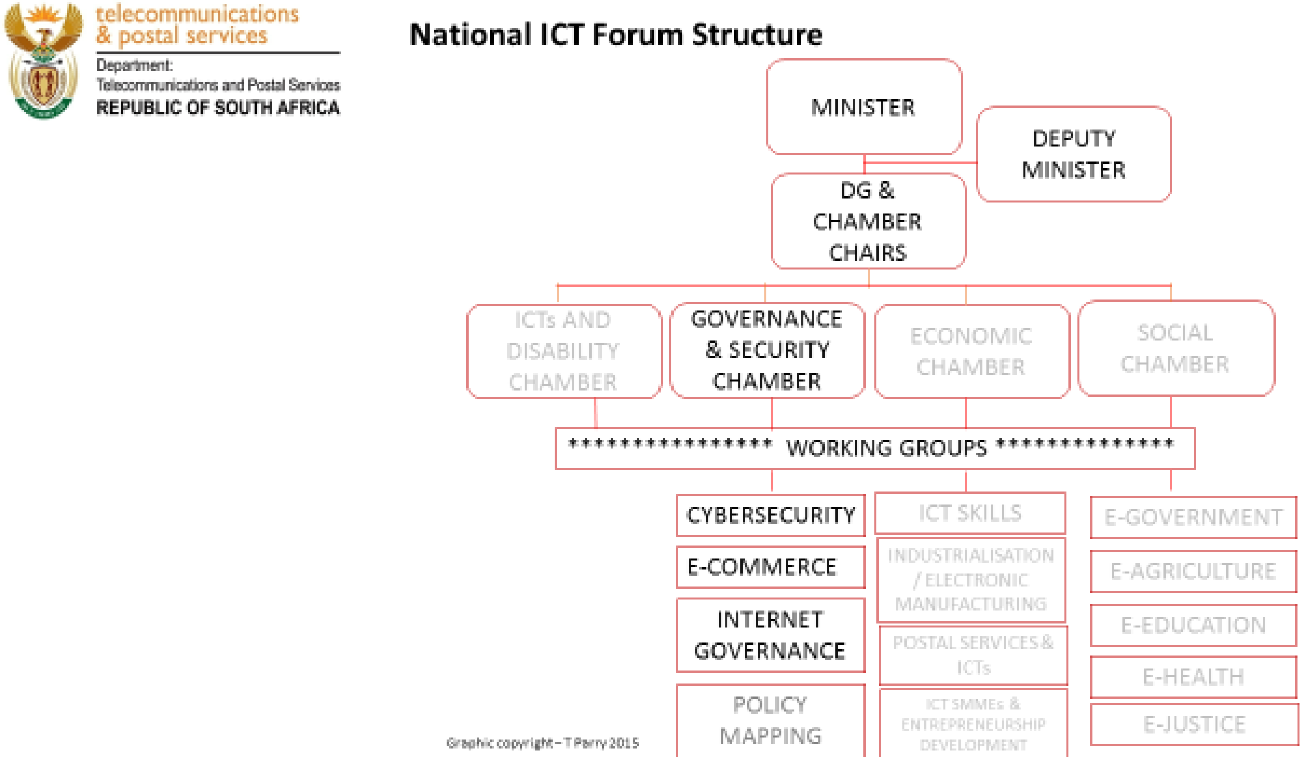
6.6.1. Social;

6.6.2. Economic;

6.6.3. Governance and security; and

6.6.4. ICTs and disability.

6.7. For purposes of this report the focus is on the Cybersecurity Working Group of the Governance and Security Chamber as per the attached diagram:


telecommunications
& postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA
National ICT Forum Structure
MINISTER
DEPUTY MINISTER
DG & CHAMBER CHAIRS
ICTs AND DISABILITY CHAMBER
GOVERNANCE & SECURITY CHAMBER
ECONOMIC CHAMBER
SOCIAL CHAMBER
**************** WORKING GROUPS ***************
CYBERSECURITY
E-COMMERCE
INTERNET GOVERNANCE
POLICY MAPPING
ICT SKILLS
INDUSTRIALISATION / ELECTRONIC MANUFACTURING
POSTAL SERVICES & ICTs
ICT SMMEs & ENTREPRENEURSHIP DEVELOPMENT
E-GOVERNMENT
E-AGRICULTURE
E-EDUCATION
E-HEALTH
E-JUSTICE
Graphic copyright – T Parry 2015

6.8. In South Africa cybersecurity is led by the Justice, Crime Prevention and Security ("**JCPS**") Cluster which is a subcommittee of Government Ministers responsible for defense and security which led to the formation of National Cyber Security Policy Framework.

6.9. The implementation of policy is coordinated by the Cybersecurity Response structure, which is a sub structure of the DGs JCPS Cluster.

6.10. The Department of Telecommunications and Postal Services ("**DTPS**") has been tasked with establishing a Cyber Incidence Response Team ("**CIRT')** – the National Cybersecurity Hub. The Hub is currently operational at pilot stage and was launched by the Minister in October 2015. One of the Hub's objectives are to promote Cybersecurity awareness.

6.11. The NCPF establishes the Cybersecurity Working Group and the purpose of the working group is to identify gaps that exist in the implementation of policies and/or legislation, and to identify challenges that lead to the non-implementation of policy, legislation and regulation in South Africa.

6.12. The country has prepared for cybersecurity through various interventions of its different respective areas of expertise. The table below provides a list of the key role players in cybersecurity within South Africa and a brief description of their respective roles.

ROLE PLAYERS	ROLES
Department of Telecommunications and Postal Services	To develop industry standards (with the assistance of ICASA and South African Bureau Standards), establish National Cyber security Advisory Council, establish Cyber security Hub, and sector specific CSIRTs.[15]
National Cyber Security Advisory Council	To advise government on Cybersecurity policies and technical issues.
CSIRT	Responsible for receiving, reviewing, and responding to computer security incident reports and activity.
Information regulator	A new regulator has been created by POPI. The role of the Information Regulator is to, amongst others, investigate complaints about alleged violations of the protection of personal information of persons to whom personal information relates.
Cybersecurity hub	The hub Acts as National point of contact for the coordination of Cybersecurity incidents, receives and analyses Cybersecurity incidents, trends, vulnerabilities and threats, facilitates the establishment of sector, regional and continental CSIRT's, disseminates alerts and warnings to its constituents and initiate national Cybersecurity awareness campaigns.
State Information Technology Agency	Sets standards for the interoperability of information systems and for a comprehensive information systems security environment for departments.
State Security Agency	Responsible for coordination, development and implementation of cybersecurity measures in the Republic as integral part of national security mandate. It must ensure that the Justice, Crime Prevention and Security cluster has the requisite capacity in relation to National Cybersecurity Policy Framework. It also hosts the Cybersecurity Response Team and Cyber security Centre.

[15] the National Cybersecurity Policy Framework 2012

Department of Justice and Constitutional Development, and National Prosecution Authority	To review various legislations governing cyberspace, harmonising and aligning them to the policy.
South African Police Services	To prevent, investigate and combat cybercrime.
Department of Defense and Military Veterans	To develop cyber defense measures to combat cyber warfare and cyber terrorism.
Department of Science and Technology and Department of Higher Education	Responsible for the development of national skills capacity as well as research and development. Training on cybersecurity to ensure South African Higher Education institutions offer cybersecurity courses. Responsible for capacity building strategy.
Department of Public Service and Administration	Developed an e-government policy: Electronic Government: The Digital Future: A Public Service IT Policy Framework. Responsible for government's overall e-government strategy in terms of the Public Service Act, 1994 (Proclamation 103 of 1994).
Presidential Infrastructure Coordinating Commission	Focuses on expanding access to communication technology and extending broadband coverage to all households by 2020 by establishing core Points of Presence in district municipalities, extending Broadband Infraco's fibre networks across provinces and ensuring penetration into rural areas.
Films and Publication Board ("**FPB**")	Sets out the regulatory framework for film and publications by means of classification, the imposition of age restrictions, and giving of consumer advice and bans the exploitative use of children in pornographic publications, films or on the internet. The FPB which was established in terms of the Films and Publications Act, no. 65 of 1996, has indicated that an amendment process is underway to allow for better regulation of online content distribution.

6.13. To this end, it is the Authority’s intention not to duplicate any role resulting in possible resource waste, however the Authority aims to focus its strength where it is mandated by the legislation.

Question 6: Taking into account the roles that are being played by different stakeholders, what additional role should the Authority play in Cybersecurity?

7. INTERNATIONAL BENCHMARKING

The cross-sector nature of cybersecurity means that various key elements of an overall cybersecurity policy will be implemented in practice through a very diverse set of institutional arrangements that differ from country to country. Furthermore, countries at different stages of development will have differing perspectives on the overall vulnerability of their country in relation to cybersecurity.

Cybersecurity approaches viewed from an economic and IT-security perspective, are often jointly led by the business community and government institutions involved in ICT development, such as the regulator or other institutions involved in the extensive use of the Internet and information technology. In other countries cybersecurity is viewed as an integral part of the fostering of an information-based economy. In those countries IT regulators play an important role not only in the implementation of cybersecurity safeguards but also in policy-making and coordination.[16]

This section examines the role that the traditional telecommunications or ICT regulators in different countries are carrying out in terms of cybersecurity. The countries were selected based on the basis of geographic diversity, different legal traditions, presence of a national cybersecurity strategy, and the availability of sources or information.

[16] Cybersecurity: The Role and Responsibilities of an Effective Regulator, 9th ITU Global Symposium for Regulators Beirut, Lebanon November 2009

7.1. South Korea

7.1.1. Before 2009, the ICT regulator known as the Korean Communication Commission ("**KCC**")[17], the National Intelligence Service ("**NIS**"), and the Ministry of Defense were tasked respectively with private sector security, national defense and protecting the safety of the government's computer system.[18]

7.1.2. As a response to an outbreak of Distributed Denial of Services[19] ("**DDOS**") attacks in 2009, the government of the Republic of Korea made its intentions public that it wanted to train three thousand cybersecurity experts as part of measures to enhance Internet security[20]. Announced by KCC, the new measures would involve setting up new departments in universities that will offer courses on information protection and provide support for the establishment of related research centres.

7.1.3. As part of the overall cybersecurity effort, the KCC would also undertake initiatives to encourage schools and companies to improve cybersecurity training and to raise awareness on Internet terrorism.

7.1.4. The KCC and the Korea Internet and Security Agency ("**KISA**") planned to have Internet service providers, such as Korea Telecom, monitor the security levels of the computers and other devices used by their customers.

7.1.5. The licensees were required to reduce the Internet connectivity of users with less-than-required software protection, thus forcing them to upgrade their existing programs or download new ones. The KCC was also granted the rights to suspend the business of software companies that fail to correct the vulnerabilities of their security programs after being ordered to do so by authorities.[21]

Question 7: What role, if any can the Authority play with regard to Cybersecurity awareness?

The KCC and the Korea Internet and Security Agency (KISA) planned to have Internet service providers, such as Korea Telecom, monitor the security levels of the computers and other devices used by their customers.

Question 8: Should the Authority strive to follow the same approach? What legislative powers are there to enable the Authority to implement this?

Question 9: Should the Authority, through the end-user regulations also require licensees to limit or cut internet connectivity of users with less-than-required software protection forcing them to upgrade their existing programs or download new ones?

Question 10: Should a legislative change be encouraged which will grant the Authority the rights to suspend the business of software companies, in the ICT sector, that fail to correct the vulnerabilities of their security programs?

Question 11: Should the mandate of the Authority be extended to software and internet regulation?

[17] Source: http://www.hani.co.kr/arti/english_edition/e_national/376585.html .

[18] http://www.antaranews.com/en/news/74600/s-korea-charts-out-national-cyber-security-strategy.

[19] Denial of service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, and DDOS is when the attempt is done by more than one source or computer.

[20] Source: Korea Communications Commission (KCC) at http://www.kcc.go.kr/

[21] Cybersecurity: The Role and Responsibilities of an Effective Regulator, 9th ITU Global Symposium for Regulators Beirut, Lebanon November 2009.

7.2. The Netherlands

7.2.1. During the World Summit on the Information Society ("**WSIS**") in 2005, spam was identified as a potential threat to the full utilisation of the Internet and e-mail. To that end, WSIS participants recognised that spam was a "significant and growing problem for users, networks and the Internet as a whole."[22] To build confidence and security in the use of ICTs, there is a need to "take appropriate action at national and international levels."[23]

7.2.2. The Dutch regulator Onafhankelijke Post en Telecommunicatie Autoriteit ("**OPTA**") deals with the problem of spam and malicious software under its wider mandate of consumer protection.[24]

7.2.3. OPTA is the authority responsible for the enforcement of anti-spam rules incorporated in the Telecommunications Act[25]. The Act implementing Directive 2002/58/EC adopts the soft "opt-in" regime. The Dutch Personal Data Protection Act also provides some protection against spam. Both OPTA and the Dutch Data Protection Authority have administrative powers. OPTA has a special website where complaints can be submitted against violators of this spam prohibition. Here you will also find general information about combating spam.

7.2.4. Spam can also be a vehicle for generating BOT[26] viruses that can lead to DDOS attacks against critical information infrastructures. Spam is therefore a potential cybersecurity risk and, in turn, a link to the concerns of policy makers concerned with cybersecurity. In this way the spam issue has become an effective vehicle for regulators to become a more integral part of national cybersecurity efforts.

[22] WSIS Declaration, paragraph 37.

[23] WSIS Plan of Action, paragraph C5.

[24] http://www.opta.nl/ Cooperation Procedure Concerning the Transmission of Complaint Information and Intelligence Relevant to the Enforcement of article 13 of the Privacy and Electronic Communication Directive 2002/58/EC, or any other applicable national law pertaining to the use of unsolicited electronic communications

Question 12: What regulatory/legislative or self-regulatory measures are in place in the regulation of spam in South Africa? What role, if any can the Authority play in this regard?

[25] Article 11.7 of the Dutch Telecommunications Act

[26] "Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information (such as web crawlers), or interact automatically with instant messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites. (http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html).

7.3. UNITED STATES OF AMERICA

7.3.1. As part of a wider national cybersecurity reassessment taking place in the United States, a comprehensive draft Cybersecurity Act 2009 was introduced. Among other matters, the draft Cybersecurity Act delegates the Federal Communications Commission ("**FCC**") with new responsibilities related to its implementation of the national broadband plan that it must develop under the American Recovery and Reinvestment Act of 2009. Under the Cybersecurity Act, the FCC is required to report on the most effective and efficient means of ensuring cybersecurity of commercial broadband networks. As part of its report, the FCC is required to consider consumer education and outreach programmes.[27]

7.3.2. The draft Cybersecurity Act also requires telecommunications carriers to take steps to ensure that customers' proprietary network information is protected from unauthorised disclosure and in this regard, the Act obliges licensees to abide by standards set by the FCC.

7.3.3. The Cybersecurity and Communications Reliability Division ("**CCR**"), a division within the FCC, works with the communications industry to develop and implement improvements that help ensure the reliability, redundancy[28] and security of the nation's communications infrastructure. CCR oversees and analyses network outage reports submitted by communications providers to identify trends in network disruptions. CCR staff then works with communications providers to facilitate improvements to communications infrastructure reliability.[29]

7.3.4. In the US, the majority of the broadband infrastructure is controlled by the private sector. The FCC is actively working with Internet Service providers and has tasked its Federal Advisory Committee, the Communications Security, Reliability, and Interoperability Council – CSRIC to develop voluntary industry-wide best practices that promote reliable networking and minimise network vulnerabilities.

[27] Cybersecurity Act of 2009 (Introduced in Senate) at http://thomas.loc.gov/cgi-bin/query/z?c111:s773:

7.3.5. USA has the highest scores in the world for the legal and capacity building pillars. One notable aspect of both capacity building and cooperation in the country is the initiatives to coordinate cybersecurity among all states. To that end, the National Governor's Association established the Resource Center for State Cybersecurity, which offers best practices, tools and guidelines.[30]

Question 12: To what extent should the Authority play a role in consumer education and outreach programmes?

Question 13: Should the Authority, through its end-user regulations require licensees to submit network outage reports to identify trends in network disruptions and as such make a report available?

Question 14: Should the Authority set similar standards for licensees to ensure that customers proprietary network information is protected from unauthorised disclosure?

7.4. NIGERIA

7.4.1. The Nigerian Communication Commission is a member of the Nigerian Cybercrime Working Group (NCWG), an inter-agency group dealing with cybercrime which has the two-fold purpose of dealing with the security of computer systems and networks as well as the protection of the critical ICT infrastructure.

7.4.2. The NCWG has established a cybersecurity forum intended to build consensus among existing agencies and provide expertise to the National Assembly in drafting new computer security legislation[31]. The working group lays the groundwork for establishing new institutional capacity in

[28] Redundancy is a process through which additional or alternate instances of network devices, equipment and communication mediums are installed within network infrastructure. It serves as a backup mechanism for quickly swapping network operations in the event of unplanned network outages.

[29] https://www.fcc.gov/encyclopedia/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-securi

[30] https://www.nga.org/cms/statecyber

[31] the Computer Security and Critical Information Infrastructure Protection Bill

Nigeria as well as for global cybercrime enforcement through relations with the Computer Crime and Intellectual Property Section of the United States Department of Justice, National High Tech Crime Center in the United Kingdom and the National Prosecuting Authority (NPA) in South Africa.[32]

7.5. MALAYSIA

7.5.1. Information security and the integrity and reliability of the network of Malaysia are identified as one of the ten national policy objectives in the Communications and Multimedia Act 1998 ("**CMA**").[33] The 10th National Policy Objective, as stated in the CMA, requires the Commission to ensure information security and the integrity and reliability of the network for the country.[34]

[32] Presentation to the ITU Regional Cybersecurity Forum for Africa and Arab States, Tunis 2009, M.U. Maska, "Building National cybersecurity Capacity in Nigeria", available at http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf

[33] Section 3 (2) (j) of the CMA of 1998.

[34] http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf

7.5.2. The CMA also regulates various activities carried out by licensees[35] as well as those using the services provided by the licensees. The CMA requires that licensees apply best endeavors to prevent network facilities or network services for, being used for the commission of any offense, prohibits fraudulent or improper use of network facilities or network services, prohibits the use or possessions of counterfeit access devices, prohibits use of equipment or device in order to obtain unauthorised access to any network services and prohibits interception of any communication unless lawfully authorised.

7.5.3. Together with the police, the Malaysian regulator, the Malaysian Communications and Multimedia Commission has enforcement powers for offences relating to network security in the CMA.[36]

Question 15: What is your understanding of networks security and how can the Authority ensure network security?

Question 16: In your understanding, how is it different from network reliability, network integrity and information security?

7.6. SWEDEN

7.6.1. In May 2002, the regulator, the Swedish National Post and Telecom Agency (PTS) established the Swedish IT Incident Centre (“**SITIC**”). Officially launched in January 2003, the SITIC supports national activities for protection against IT incidents by:

[35] Network facilities providers, network service providers, applications service providers and content applications service providers.

[36] Malaysian Communications and Multimedia Commission (MCMC) at http://www.skmm.gov.my/

7.6.1.1. Operating a system for information exchange on IT incidents between public and private organizations and the SITIC;

7.6.1.2. Operating a public warning system providing information on threats to IT systems;

7.6.1.3. Providing information and advice on security and counter measures;

7.6.1.4. Compiling and publishing incident statistics.[37]

Question 17: Should the Authority assume some functions done by SITIC and if so, how should the Authority be resourced?

[37] Swedish IT Incident Centre (SITIC) at http://www.sitic.se/

7.7. UNITED KINGDOM

7.7.1. Get Safe Online is a public and private sector joint campaign to raise awareness of online security aimed at the general public and small businesses. Get Safe Online is sponsored by the United Kingdom Cabinet Office, the United Kingdom Office of Communications ("**Ofcom**"), the Serious Organised Crime Agency ,Microsoft, HSBC, Cable & Wireless, and Paypal.

7.7.2. The Get Safe Online initiative works with a range of community organizations and aims to give people the confidence to go online securely. The initiative coordinates marketing and public relations activities as well as providing a comprehensive website with up-to-date advice, tools and guidance on general internet security. The website includes information on protecting individuals, families and businesses online, as well as advice on topics such as Internet shopping, social networking sites, data theft and identity fraud.

7.7.3. In 2014 Ofcom published a report for Government outlining measures put in place, by UK's largest internet service providers, to help parents protect children from harmful content online.

7.7.4. This was followed by an agreement between the Government and BT, Sky, TalkTalk and Virgin Media, the four largest fixed line internet service providers ("**ISPs**"), announced in July 2013. Each ISP committed to offer new customers 'family-friendly network-level filtering' by the end of December 2013.

7.7.5. This was the second of three reports on internet safety measures to protect children produced by Ofcom, at the request of the Department for Culture, Media and Sport ("**DCMS**"). The DCMS asked Ofcom to look at the approach taken by each ISP to implement family-friendly filtering services which block content that may be inappropriate or harmful for children, rather than assess the effectiveness of the filters.

7.7.6. The report also describes measures taken by ISPs to present a pre-ticked 'unavoidable choice' to new customers on whether or not to activate the filter, and includes initial take-up data among new customers offered filters.[38]

Question 18: What cybersecurity measures are in place by ISPs in South Africa to protect the consumers?

Question 19: Should the Authority require licensees to offer new and/or all customers 'family-friendly network-level filtering?

7.8. MAURITIUS

7.8.1. In terms of the survey produced by the International Telecommunication Union ("**ITU**") that measures the commitment of Member States to cybersecurity in order to raise awareness, Mauritius is the top ranked country in the Africa region. It scores particularly high in the legal and the technical areas. The Botnet Tracking and Detection project allows Computer Emergency Response Team of Mauritius to proactively take measures to curtail threats on different networks within the country. Capacity building is another area where Mauritius does well. The government IT Security Unit has conducted 180 awareness sessions for some 2000 civil servants in 32 government ministries and departments.

Question 20: Can Botnet Tracking and Detection help in threats on the network in South Africa? If yes, who must do it and how? How can the Authority get involved in this?

[38] http://media.ofcom.org.uk/news/2014/internet-safety-measures/

7.9. RWANDA

7.9.1. Rwanda ranked second in Africa and scored high in the organisational pillar and has a standalone cybersecurity policy addressing both the public and private sector. It is also committed to develop a stronger cybersecurity industry to ensure a resilient cyber space. [39].

7.10. KENYA

7.10.1. Kenya ranked third in Africa, provides a good example of cooperation through its National Kenya Computer Incident Response Team Coordination Centre.[40] The CIRT coordinates at national, regional and global levels with a range of actors. Nationally this includes ISPs and the financial and educational sectors; regionally it works with other CIRTs through the East African Communications Organization; and internationally it liaises with ITU, Forum of Incident Response and Security Teams, and bi-laterally with the United States and Japan CIRTs among others.

7.11. CANADA

7.11.1. Canada ranks second in the North American region with its highest score in the legal pillar. The country's Personal Information Protection and Electronic Documents Act features several sections relating to cybersecurity.[41] It requires organizations to notify privacy authorities in the event of privacy breaches that could cause significant damage with penalties for those who fail to report them.

[39] http://www.myict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01. pdf

[40] http://www.ke-cirt.go.ke/index.php/members/.

[41] http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Question 22: Is POPI sufficient to deal with protection of Personal information. What can ICASA do to help enforce POPI in the ICT sector?

7.12. MEXICO

7.12.1. Mexico is third behind Canada, illustrating the cybersecurity divide in the North American region. Like the other top ranked countries in the region, it scores best in the legal pillar with a full suite of cyber legislation covering criminality, data protection, data privacy and electronic transactions.

7.13. SULTANATE OF OMAN

7.13.1. Oman is the top ranked in the Arab States with the highest scores in the legal and capacity building pillars. Oman has a robust organizational structure, including a high-level cybersecurity strategy and master plan and comprehensive roadmap.

7.14. EGYPT

7.14.1. Egypt ranks second in the North East African region with a full range of cooperation initiatives. It is a member of the UN Government Group of Experts on cybersecurity[42], has chaired the ITU Working Group for Child Online Protection,[43]was a founding member of AfricaCERT,[44] and has a number of bi-lateral and multilateral agreements on cybersecurity cooperation.

[42] https://www.un.org/disarmament/topics/informationsecurity/

[43] http://www.itu.int/en/council/cwg-cop/Pages/default.aspx

[44] https://www.africacert.org/home/

Question 23: Should ICASA be involved with Online Child Protection? If so, how?

7.13. QATAR

7.13.1. **Qatar** ranks third in the Middle East and has been building a cybersecurity culture through campaigns such as Safer Internet Day and has spread warnings about online threats, such as fraud and Internet scams, via print and social media. The Qatar Cyber Crimes Investigation Center and Information Security Center support efforts to safeguard the public and crack down on those who use technology to carry out criminal activities.

7.14. SINGAPORE

7.14.1. **Singapore** is the top ranked country in the region. The island state has a long history of cybersecurity initiatives. It launched its first cybersecurity master plan back in 2005. The Cyber Security Agency of Singapore was created in 2015 as a dedicated entity to oversee cybersecurity and the country issued a comprehensive strategy in 2016. [45]

7.15. MALAYSIA

7.15.1. Malaysia is ranked second in the Asia and the Pacific region and scores high on capacity building due to a range of initiatives in that pillar. Cybersecurity Malaysia, the government entity responsible for information security in the country, offers professional training through higher education institutions in Malaysia. It maintains the *Cyberguru* website, dedicated to professional security training[46].

[45] https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

[46] http://www.cyberguru.my

Question 24: How can ICASA be involved in offering of professional cybersecurity training to primary, secondary and tertiary institutions of learning?

7.15. AUSTRALIA

7.15.1. Australia is third ranked in the region and home to AusCERT, one of the oldest CERTs in the region formed in 1993.[47] The highest scoring pillar is technical where there is a certification programme for information security skills provided by the Council of Registered Ethical Security Testers ("**CREST**").[48] Modelled after CREST, the council offers assessment, accreditation, certification, education and training in cyber and information security for individuals and corporate entities in both Australia and New Zealand.

7.16. GEORGIA

7.16.1. Georgia is top ranked in the Commonwealth of Independent State (CIS). After large -scale cyber-attacks on the country in 2008, the government has strongly supported protection of the country's information systems.[49] The Information Security Law[50] established a Cyber Security Bureau with a particular emphasis on protecting critical information systems in the military sphere.

[47] https://www.auscert.org.au.

[48] https://www.crestaustralia.org.

[49] http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx?lang=en-US.

[50] https://matsne.gov.ge/en/document/view/1679424.

7.17. THE RUSSIAN FEDERATION

7.17.1. Russia ranked second in the Northern Asia region, and scored the highest in capacity building. Its commitments range from developing cybersecurity standards to Research and development strategies ("**R&D**") and from public awareness to a home-grown cybersecurity industry. An example of the latter is Kaspersky Labs, global cybersecurity company, founded in 1997 and whose software protects over 400 million users and some 270 000 organisations.[51]

Question 25: Do you think ICASA should be involved in Cybersecurity standards, research and development and/or home-grown cybersecurity industry? If yes, please elaborate how on each of the above category

7.18. BELARUS

7.18.1. Belarus is the third ranked country in the post-Soviet countries, where child protection initiatives include public and private partnerships. Mobile operator MTS has implemented a project with the Ministry of Education to teach children about safe Internet practices that has so far reached some 6000 children.[52]

Question 26: How can Mobile operators partner with ICASA to teach children about safe Internet practices?

[51] https://usa.kaspersky.com/about.

[52] http://www.mts.by/news/97338/.

7.19. ESTONIA

7.19.1. Estonia is the highest-ranking nation in the Europe region. Like Georgia, Estonia enhanced its cybersecurity commitment after a 2007 attack. This included the introduction of an organizational structure that can respond quickly to attacks as well as a legal act that requires all vital services to maintain a minimal level of operation if they are cut off from the Internet.[53] The country also hosts the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence.[54]

7.20. FRANCE

7.20.1. France is the second highest ranked in Europe, scoring a perfect 100 in capacity building. There is widespread cybersecurity training available in the country, and the National Agency for Information System Security (ANSSI in French) publishes a list of dozens of universities that provide accredited cybersecurity degrees recognized.[55]

Question 27: How can ICASA partner with tertiary institutions to help them provide accredited cybersecurity qualifications?

[53] http://www.nextgov.com/cybersecurity/2015/01/heres-what-us-could-learn-estonia-about-cybersecurity/103959/

[54] https://ccdcoe.org

[55] https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/

8. PROPOSED CYBERSECURITY APPROACH FOR THE AUTHORITY

The Authority as an ICT regulator intends to play a significant role in the national cybersecurity effort of the country. While cybersecurity is a shared responsibility of government, the private sector and individuals alike, the Authority recognises that only national government is in a position to lead a collective nation cybersecurity effort. However, given the constantly changing ICT environment and the dynamics of cybersecurity, the role of the Authority has to be assessed and if there is a need for evolution it should be applied. The Authority has identified the following areas where it can play a role. As previously stated these are the Authority's initial view and the Authority intends to be inclusive of affected stakeholders in coming up with decisions.

8.1. PRIVATE SECTOR COOPERATION AND INDUSTRY REGULATION

8.1.1. The Authority has the mandated powers to engage the private sector in policy consultations and to promote industry regulation. This positions the Authority to lead cybersecurity coordination and cooperation activities that involve the private sector and industry.

8.1.2. The following lists the regulatory approach that the Authority wishes to consult on for industry regulation:

8.1.2.1. Encourage public-private sector efforts to develop cybersecurity standards, procedures, and codes of conduct;

8.1.2.2. Mandate or encourage the adoption of international cybersecurity standards (e.g. ISO 27001 on Information Security Management System) and recommend best practices; and

8.1.2.3. Ensure the integrity of the main pipelines for delivery of ICT services is a key component of an overall cybersecurity program.

8.1.3. Sections 35 and 36 of the ECA mandates the Authority to prescribe standards for the performance and operation of any equipment or electronic communication facility, aimed at, among others, protecting the integrity of the electronic communications network. The Authority in protecting the integrity of the electronic communications network, should consult with stakeholders on the understanding of what it means to protect the integrity of the network.

Question 28: Is integrity as written in ECA equivalent to security? Please elaborate

Question 29: Do you agree with the proposed regulatory interventions? Please elaborate

8.2. CAPACITY BUILDING

8.2.1. A lot of cybersecurity vulnerabilities exist because of a lack of cybersecurity awareness and access to resources to manage cybersecurity on the part of end-users. There arises a need to promote a culture of cybersecurity thus increasing the level of cybersecurity competence in general.

8.2.2. It is the Authority's view that capacity building may be promoted by requiring the licensees to take efforts to train personnel and to adopt widely-accepted security certifications. Cyber safety has to be an integral part of the use of ICT products and services.

8.2.3. Consumer protection forms an integral part of the Authority's regulatory mandate, for years the Authority has been involved in the organisation and implementation of consumer awareness initiatives that involve communications through a range of channels. The same channels of communication may be used for communicating materials and information on cybersecurity.

Question 30: What measures do licensees have in place to capacitate the consumer on issues of cybersecurity awareness?
Question 31: Should the Authority place requirements on licensees to capacitate and make consumers aware of cyber related threats? Please elaborate.

8.3. POLICY MAKING

8.3.1. The responsibility for ICT policy making is delegated to the legislature and administered by the Parliament in South Africa. However, the Authority can play a key role in policy-making by virtue of its familiarity with the sector that it regulate, resources available to the regulator, and the processes and mechanisms that have been put in place to engage in consultations with industry stakeholders.

8.3.2. With cybersecurity being increasingly recognised as a prominent ICT-related issue, the Authority's policy advisory functions should increasingly be required to provide inputs on cybersecurity issues. With the introduction of Next Generation Networks and the market regulation thereof, the Authority intends to begin examining the cybersecurity dimension of the introduction of such networks and the security interventions that the Authority can employ.

Question 32: What policy-making role should the Authority play with regards to Cybersecurity?

8.4. REGULATING CYBERSECURITY STANDARDS

8.4.1. As mentioned in paragraph 5.5 above, the mandate of the Authority is derived from the ECA and there are basically three cybersecurity variables that the ECA identified and requires the Authority to fulfill, which are network reliability, network integrity and information security:

8.4.1.1. Network reliability

8.4.1.1.1. Network reliability is fulfilled by the Type Approval Regulations 2013,[56] End-user and Subscriber Service Charter Regulations 2016,[57] as well as the revised official list of Regulated Standards for Technical Equipment and Electronic Communications Equipment Regulations.[58]

8.4.1.1.2. To fulfill this mandate, the Authority has established an MoU with the SABS to this effect and as a result of this MoU, electronic equipment that fall under the mandate of ICASA is subjected to robust conformity assessment procedures to ensure that such products meet the quality requirements as stipulated in the South African National Standards.

8.4.1.1.3. The Authority has, among other things, adopted many technical standards by the European Telecommunications Standards Associations for equipment as required by the ECA.

8.4.1.2. Network integrity and Information security

8.4.1.2.1. The role that the Authority should play in the development or adoption of standards is explicit in the NCPF. The framework expressly states that it promotes the development and/or adoption of standards by the SABS in consultation with relevant Government Departments, ICASA and the industry. This will ensure a safe and secure cyberspace environment that will enable the growth of e-commerce and an inclusive information society.

8.4.1.2.2. The advent of the Internet of things, where machines were built for services and not with security in mind requires the development or adoption of minimum security standards for these equipment before they may be approved.

8.4.1.2.3. The Authority does not intend to apply overenthusiastic measures at this stage as this may result in unduly onerous requirements on licensees, which in turn may affect market entry and the introduction of services.

8.4.1.2.4. Through this Discussion Document, the Authority wishes to consult with stakeholders. Depending on the outcome of the Discussion Document it may be that instead of formal regulation, the Authority may develop means of safeguarding for cybersecurity such as issuing of best practice guidelines, or through self-regulation initiatives taken through public-private sector forums.[59]

Question 33: What cybersecurity standards should the Authority require licensees to comply with?
Question 34: Is self-regulation sufficient in the area of cybersecurity? How is this implemented? How is it monitored?
Question 35: Are there any other issues that the Authority should be aware of in relation to ICT regulators and cybersecurity?

[56] Published under General Notice 871 in *Government Gazette* 36785 of 26 August 2013 as amended.

[57] Published under General Notice 189 in *Government Gazette* 39898 of 1 April 2016 as amended.

[58] Published under General Notice 603 in Government Gazette 39182 of 9 September as amended

[59] https://www.atkearney.com.au/paper/-/asset_publisher/dVxv4Hz2h8bS/content/internet-value-chain-economics/10192. Source: A.T. Kearney analysis

9. CONCLUSION

9.1. Cybersecurity is an important aspect of National Security and the safekeeping of South Africa's constituency and resources.

9.2. The actual role the Authority can and should play, depends on a number of variables. In particular, the question of how cybersecurity and cyber threats are perceived as a nation is usually a key determinant of how cybersecurity roles and responsibilities are assigned among government institutions, with a technical, technological ICT focused perception of the problem being the most favourable to a large role for regulators.

9.3. The Authority intends to adopt a flexible and adaptive approach to its cybersecurity efforts as threats to cybersecurity are constantly evolving. With the role that the Authority plays in this current ICT environment, it has found itself well positioned in terms of mandate, resources and experience to deal with current and emerging cybersecurity challenges. With many stakeholders participating in the cybersecurity space, it becomes imperative that the Authority performs its mandate with regard to information security and network integrity.

9.4. The Discussion Document serves as the first step of consultation with stakeholders in the sector. Following the publication of the Discussion Document the public will be given an opportunity to submit comments. Should it be deemed necessary, a public hearing will be convened and thereafter a Findings Document will be published.