SENTECH'S

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

30 NOVEMBER 2018

Head Office: Sentech Technology Park (STP), Octave Street, Honeydew, 2040
Postal Address: Private Bag X06, Honeydew, 2040
Telephone: 011 471 4400 | Call Centre: 0860 736 832 (International: +2711471 4595)
Fax: 011 294 2670 | E-mail: support@sentech.co.za | www.sentech.co.za

SENTECH
connecting You

Table of Contents

1. Introduction

SENTECH thanks the Independent Communications Authority of South Africa ("Authority") for the opportunity to make a written submission on the *Inquiry into the role and responsibilities of the Independent Communications Authority of South Africa in Cybersecurity*.

2. Inquiry questions and answers

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

2.1.1. Answer to question 1

The answer is simply yes. Historically regulatory reforms have been a consequence of the following, inter alia: 1) adoption and diffusion of technology as a consequence of the decreasing costs in implementation; 2) democratization of regulatory frameworks through the creation of independent regulators; and 3) technology convergence and pro-competition regulatory frameworks. The 4th industrial revolution has enforced ICT regulatory reform as a consequence of the transformational nature of communications, the fast evolving technological environment and the increase in mass personalised production. The transformation has created a 4th generation regulator whose task has been expanded beyond addressing traditional issues with regards to technology convergence and competition issues (inter-licensees and/or versus unlicensed operators). But also to address socioeconomic issues of social growth, social inclusion, economic growth, social development, etc. Figure 1 below illustrates the scope of the 4th generation regulator as a consequence of socioeconomic policies.

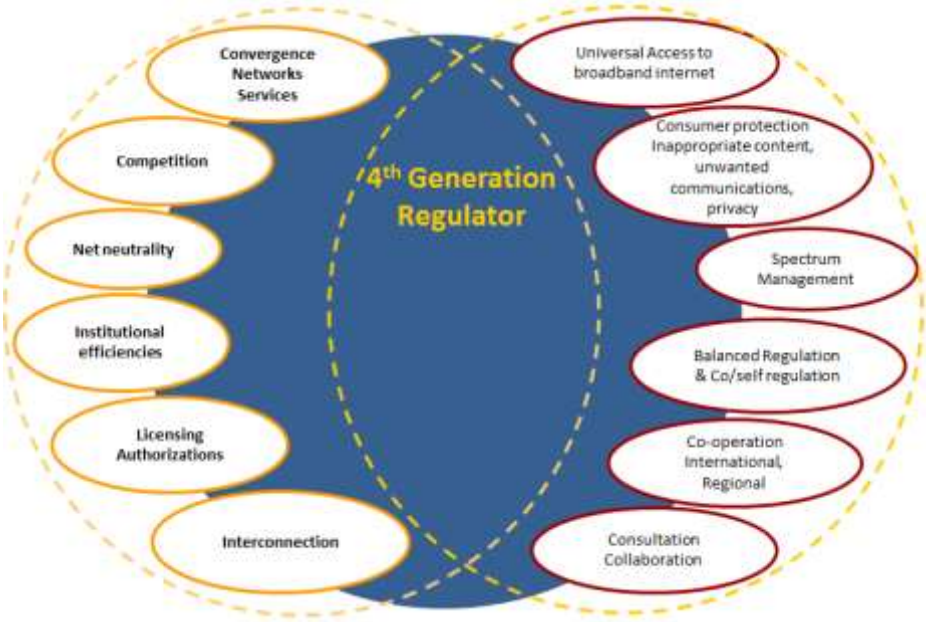

Figure 1: 4th Generation Regulator (source: ITU)

It is also important to acknowledge global frameworks used to measure country's developmental progress when discussion issues relating to evolving regulatory functions. For example the ITU ICT development Index (IDI). Socioeconomic ICT policies such as the Department of Telecommunications and Postal Services': *National Integrated ICT Policy White Paper (2016)*, at heart seeks to influence South Africa's indicators used by the ITU to bench measure the countries ICT Development Index (IDI). IDI is used to measure and compare South Africa against other countries in reference to developments in ICTs. Figure 2 below demonstrates the conceptual framework used by the ITU for the IDI model. The model looks at four measures: 1) the level of infrastructure deployment and the extent of access to ICTs; 2) the level of diffusion of the Internet, fixed and mobile broadband; 3) the everyday usage of ICTs for educational, economic, social needs and knowledge creation; and 4) the developmental and socioeconomic impact of the combination of access, usage and skills.

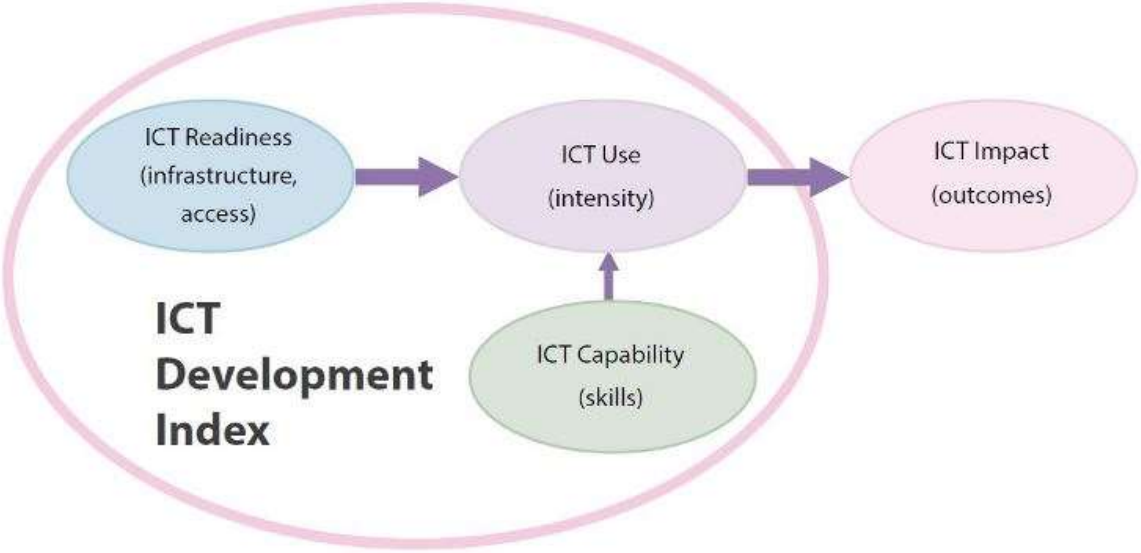

Figure 2: Stages in the evolution towards an information society (source: ITU)

The extent of influence of the 4th generation regulator and socioeconomic policies as measured via the ICT Development Index (IDI) speaks to the attainment of United Nations' Sustainable Development Goals (SDGs), figure 3, through the deployment and use of technology. The UN declared the internet a human right mainly as a consequence of how the service has become a "non-optional utilit[y] whose availability and performance impact every aspect of the economy and societal development" (ITU, 2016).

Figure 3: United Nations' Sustainable Development Goals (SDGs)

Access to the Internet is crucial to a fully functional human as the service enables access to other rights such as freedom of access to: health care; education; information; speech; association; political participation; etc. For example, the Gauteng Department of Education has introduced an online system for school

registration. Consequently, communities and individuals with limited access and/or competence/skills of the Internet are placed at a disadvantaged position. It is on this basis that digital literacy positively influences technology diffusion.

It is also important to note that one of the core services to the all-inclusive and successful implementation of the 4th industrial revolution is the Internet. The extent of freely available information has made the Internet a fundamental tool for the democratisation of information and education. The Internet is also an essential tool for creating economic opportunities and, creation of mass access to education regardless of socioeconomic issues and geographic displacement.

The importance of access to the internet in relation to human's ability to be fully functional on a daily basis can never be overstated. Taking into consideration Maslow's motivational psychological theory: A Theory of Human Motivation, it is not surprising that there are arguments insisting on the inclusion of access to the internet as a basic human needs to be met, as a motivation for the achievements of higher and more complex needs. The bottom of the pyramid represents the most basic needs.

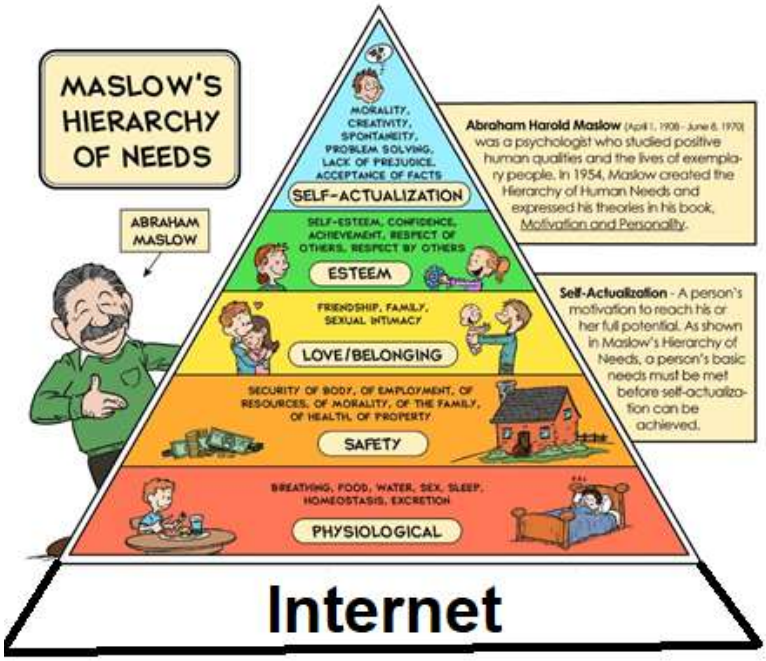

Figure 4: Maslow's Hierarchy of needs

2.2. Question 2: How would you define cybersecurity?

2.2.1. Scope of information security with respect to the EC Act

As stated correctly by the Authority, subsection 2(q) of the EC Act empowers ICASA to develop regulations on information security with respect to electronic communications (analogue and digital). Therefore the Authority is empowered to make regulations in relation to the protection of information "from unauthorized access, use, disclosure, disruption, modification, inspection, recording or

destruction”[1] in respect to confidentiality, integrity and availability of the information. Information security includes the following formats, *inter alia*; documents, intellectual property, verbal or visual communications in digital or any other format.

Taking into consideration the formats included in information security and the intention of subsection 2(q) of the EC Act, it is very clear that the Authority is limited to developing regulations with respect to the electronic format of information carried through electronic communications network.

Section 2(q) of the EC Act:

2 *The primary object of this Act is to provide for the regulation of electronic communications in the Republic in the public interest and for that purpose to—*

(q) ensure information security and network reliability;

Definition of electronic communications

"electronic communications" *means the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electromagnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service*;

2.2.2. Cybersecurity

SENTECH support the arguments that cybersecurity is a subset of information security and that the two (2) terms are not interchangeable. SENTECH supports the view that cybersecurity is concerned with information or things impacted by the vulnerability of electronic communications. Cybersecurity also considers processes, technologies and practices deployed to store, analyse, transmit and secure information, including other things such as appliances, cars, road management systems, etc. Figure 5 illustrates the difference between information and cybersecurity.

[1] https://www.secureworks.com/blog/cybersecurity-vs-network-security-vs-information-security

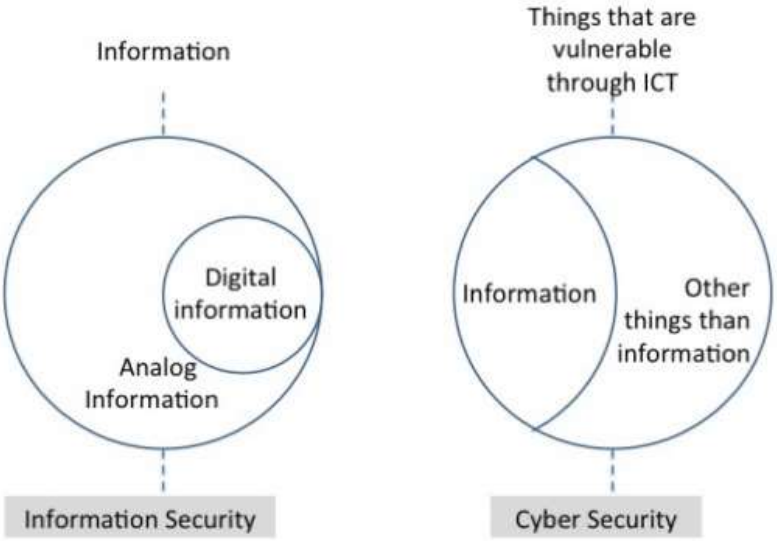

Figure 5: Differences between information and cybersecurity[2]

2.2.3. Answer to question 2: defining cybersecurity

When seeking to define cybersecurity, it is important to first determine whether South Africa does not have existing definition in either Policy and/or Legislation. As it is known by the Authority, Parliament has recently (27/11/2018) voted on the Cyber Crime Bill. Though initially the Bill included both cybercrime and cybersecurity the final document excluded two (2) chapter, namely on Structures to deal with cybersecurity and Critical information infrastructure protection, from the final Bill. It is currently not clear how the excluded two (2) chapters will be dealt with going forward.

The Bill initially had a definition for cybersecurity, since the principle is no longer included, SENTECH supports the adoption of the definition as stated in the National Cybersecurity Policy Framework ("National Framework") as gazetted on 04 December 2015, government gazette no. 39475. Taking into consideration that there are varying definitions of cybersecurity, the supported definition is most importantly tied to the National Framework.

2.3. Questions 3 and 4:

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

[2] www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information

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?

2.3.1. Answer to questions 3 and 4

Taking into consideration the National Framework and Cybercrime Bill, SENTECH advocates for the Authority to consult with the Department of Telecommunications and Postal Services ("DTPS") regarding the Regulator's role with respect to Cybersecurity. SENTECH acknowledges and respects the Authority's independence.

SENTECH acknowledges that the EC Act was conceptualised during a period it was not possible to forecast the extent of the impact of the use of the Internet. It is also important to acknowledge that all amendments made of the EC Act did not address issues of Cybersecurity. The proposal for the Authority to consult with the DTPS takes into consideration the extent at which cybercrime and cybersecurity affects every tier of government.

2.4. 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.

2.4.1. Answer to question 5

The standards referred to in Section 36(2) of the EC Act relate to electronic communications equipment used for the provisioning of the network and services, such as end user equipment etc.

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

2.5.1. Answer to question 6

SENTECH advocates for the Authority to not necessarily seek any additional role to play, but as stated prior to consult with the DTPS in reference to the National Framework.

2.6. Question 7 and 8

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?

2.6.1. Answer to question 7 and 8

The National Framework is clear on issues of objectives and responsibilities, it is therefore not advisable for the Authority to seek to operate outside this framework. It is also important to note that South Africa's experience on issues of cybercrime and cybersecurity are unique consequent of the country's status quo on the diffusion of the Internet and applications dependent on the Internet. Therefore the country's policy/legislative/regulatory frameworks will better advice on how to address issues of cybercrime and cybersecurity. It is also crucial to acknowledge the importance of benchmarking, but the outcome of this process must take into consideration the country's existing policy/legislative/regulatory frameworks.

2.7. 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?

2.7.1. Answer to question 9

SENTECH is of the view that the Authority will be operating outside their mandate and should therefore not consider the proposal. The issues of end-user equipment is mainly addressed through software upgrades suggested by

manufacturers of end-user equipment and the issue of upgrades is linked costs, namely connectivity fees. It is also not clear who the Authority envisions will determine what is meant by “less-than-required software protection”.

2.8. 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?

2.8.1. Answer to question 10

The simple answer is NO. The Authority already has a lot to deal with and the Regulator has previously highlighted issues of not being appropriately funded. The Authority should concentrate mainly on matters relating to the International Telecommunications Union (“ITU”).

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

2.9.1. Answer to question 11

It is not clear why the Authority is considering the issue of Internet regulation and it is also not stated what the Regulator considers as Internet regulation. SENTECH advocates for the Authority to not seek to operate outside the EC Act. Issues of Internet regulations are partly mandate of the Films and Public Board & also covered in the National Framework.

2.10. Question 22: Should the mandate of the Authority be extended to software and internet regulation?

2.10.1. Answer to question 22

The Information Regulator has not been operating for long enough to determine their effectiveness. It is also important to note that the Authority’s question can never be addressed without referencing both the POPI Act and the Information Regulator. This also SENTECH believes is not within the mandate of the Authority.

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

2.11.1. Answer to question 23

The issues of online child protection is part of the responsibility of the Films and Publication Board. This is another aspect outside the mandate of the Authority.

In order to avoid repetition, questions 24, 25, 27, 30, 31, 32, 33, 34 and 35 fall outside the mandate of the Authority. The National Framework addresses these issues.

3. Conclusion

SENTECH thanks the Authority for the opportunity to make representations on the enquiry.