Governing an Internet of Risks

Submission to the Inquiry into the role and responsibilities of the ICASA

Enrico Calandro (PhD)
Public Hearings, Centurion, South Africa | 16-17 January 2019
How RIA approaches digital policy

cybersecurity
- resilience, security, trust, data protection

access and use+
- supply side (infrastructure, pricing, QoS); demand side (affordability, skills, content, e-literacy)

digital economy
- e-work, e-finance, e-trade, e-taxation

innovation
- AI, blockchain

human rights
- gender

regulation
capacity-building
dissemination
governance
collaboration
evaluation
collaboration

After Access surveys
An Internet of Opportunity and Risk
Digital inequalities

Gender

Location

Source: 2017 #AfterAccess surveys
Cyber-incidents

2017 #AfterAccess survey data

Have you ever experience cyber-incidents? (% of Internet users)

<table>
<thead>
<tr>
<th>Country</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Africa</td>
<td>10</td>
</tr>
<tr>
<td>Kenya</td>
<td>11</td>
</tr>
<tr>
<td>Nigeria</td>
<td>11</td>
</tr>
<tr>
<td>Mozambique</td>
<td>14</td>
</tr>
<tr>
<td>Tanzania</td>
<td>15</td>
</tr>
<tr>
<td>Ghana</td>
<td>15</td>
</tr>
</tbody>
</table>

Level of education of cyber-incidents victims (%)

<table>
<thead>
<tr>
<th>Education Level</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>Primary</td>
<td>7</td>
</tr>
<tr>
<td>Secondary</td>
<td>10</td>
</tr>
<tr>
<td>Tertiary: Diploma/Cert</td>
<td>12</td>
</tr>
<tr>
<td>Tertiary: Bachelors</td>
<td>15</td>
</tr>
<tr>
<td>Tertiary: Masters</td>
<td>34</td>
</tr>
<tr>
<td>Tertiary: PhD</td>
<td>54</td>
</tr>
</tbody>
</table>
Setting the scene: Defining cybersecurity

- **Human-centric approach**
- **Technological and organizational perspective**
- **Telecommunications/ICT security**
- **2012 NCPF ITU**

**Techno-centric + normative approach**
Setting the scene: Defining cybersecurity

Technological and organizational perspectives (1/3)

- Cybersecurity means different things to different stakeholders.
  - from a **technological perspective**, it refers to technologies developed to safeguard computer systems and the information stored on such systems.
  - from an **organizational perspective**, it 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.
Setting the scene: Defining cybersecurity

Definition adopted in South Africa (2/3)

- 2012 National Cybersecurity Policy Framework (NCPF): adopted the ITU Definition of cybersecurity
  - Need for adopting a multi-sectoral and multi-disciplinary approach to improve the resilience of information systems against attacks and accidental damages
  - The approach encompasses strategic, legal, regulatory, as well as technological and non-technological mechanisms
    - Aim: protecting different elements of the Internet infrastructure, end-user devices, and other connected devices.
Setting the scene: Defining cybersecurity

Telecoms security (3/3)

- Measures and controls taken to ensure the **security of information being transmitted** by telecommunications networks and the **security of telecommunications networks and infrastructures**.

- Implies the application of security measures to telecommunications systems, and regulatory interventions, 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.
Telecommunications networks: necessary backbone for the exchange of communication between electronic communication devices (computers, mobile and others). 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.

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

(1/4) Global Context

‣ 2017 Global Cybersecurity Index: South Africa ranked 58th globally and 6th in Africa
  • Preceded by Mauritius, Rwanda, Kenya, Nigeria, and Uganda

‣ Signatory of 2014 AU Convention on Cyber Security and PDP; 2011 Budapest Convention on Cybercrime
  • Not Ratified
2012 National Cyberpolicy Framework

- Set-out measures and mechanisms for coordination across government. It mandated the DTPS to establish a National Cybersecurity Hub: central point for collaboration between the industry, government, CSO on all cybersecurity incidents

Problems:

- Implemented slowly
- Involvement of many organisations and links into more structures suggest problematic coordination between rivalrous ministers

Do we have the admin and technological skills to deliver?
Context

(3/4) National Legislative Framework on Cybersecurity

‣ National Foundational Legislation of cybersecurity
  • 2002 Electronic Communications and Transactions Act
  • 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act
  • 2009 Protection of Personal Information (enacted in 2013)

‣ 2015 National Cybersecurity Framework
  • Draft Cybercrime and Cybersecurity Bill
  • 2018 Cybercrime Bill
Institutional Design Dealing with Cybersecurity

State Security Agency

Minister of Justice

Cabinet Justice, Crime Prevention and Security Cluster JCPC Cluster

Director General of State Security

Cyber Response Committee (CRC)

DTPS

National Cybersecurity Hub
Problems of the current institutional arrangement

- Poor mechanisms for information flow regarding cybersecurity in govt depts

- Potential for limited transparency or oversight – Cybersecurity Response Committee in charge of strategy and decision-making, is chaired by the Director-General of State Security

- 2017 Draft Communications Act Amendment Bill suggests to merge ICASA, the USAASA, and .ZADNA in a new Economic Regulator under the newly merged MoC and DTPS

- Concerns on the powers, competencies and independence of ICASA
Research on cyber readiness, cyber-risks, and cyber incidents

Government organisations

- 2017 DTPS Cyber Readiness Report: 3 top challenges facing organisations in ZA with regards to cybersecurity were:
  - Insufficient skills (57%); lack of in-house skills (49%); and lack of awareness of cyber risks (39%)

Research on cyber readiness, cyber-risks, and cyber incidents

Internet measurement platforms

- **Oracle Dyn**: data on BGP hijack detection
- **Thousandeyes**: DDoS monitoring
- **Akamai’s State of the Internet Security** and **Cisco’s Annual Cybersecurity Report**: Commercial reports. Offer insights into citizens and firms experience but offer little information about South Africa
- **Symantec’s Internet Security Threat Report**: comprehensive collection of data on cyberthreats data
- **CyberGreen**: provides levels and trends of risk posed to others by the country
Research on cyber readiness, cyber-risks, and cyber incidents

Primary and Secondary research

- National representative data: RIA #AfterAccess survey
  - 6.81% of internet users have been conned over the Internet and lost money
  - 10% of internet users had their account hacked
  - 3.93% of Internet users >16 y-o have experienced cyber bullying

- Secondary data research: Van Niekerk (2017), recorded a total of 54 cyber incidents spanning 23 years from April 1994 to end 2016
  - Most of the incidents had an impact on data exposure, in addition to advanced persistent threat (APTs) infections, including cyber espionage
Recommendations: 1 – Research and development

- Research on cybersecurity is increasingly being conducted
  - Growing number of existing and new organisations are monitoring cyber threats and cyber incidents in South Africa.
- 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.
Recommendations: 1 – Research and development

Considering the complexity of measuring threats, risks, and harms in cyber contexts, 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.
Recommendations:

2 – Cyber Maturity Assessments

- Conducted to obtain empirical, independent, and impartial evaluation of the cyber maturity level of the country

  - 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

GCSCC, Oxford: 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 & Strategy; 2) Cyber Culture and Society; 3) Cybersecurity Education, Training, and Skills, 4) Legal and Regulatory Frameworks; 5) Standards, Organisations, and Technologies
Recommendations: 3 – Developing a National Cybersecurity Strategy

Lessons on private sector cooperation and industry regulation

- Mauritius
  - National Cybersecurity Strategy implemented through a collaborative arrangement which extends to public and private sector entities and stakeholders from different sectors
  - ICTA: one of the main stakeholders across all projects of the Action Plan of the National Cybersecurity Strategy, and is involved in a number of projects dealing with securing cyberspace
  - ICTA is also involved in the development and implement of a CIIR framework and in cyber crisis management plan
Recommendations: 3 – Developing a National Cybersecurity Strategy

Lessons on private sector cooperation and industry regulation

- Ghana
  - National Cybersecurity Policy and Strategy: NCA has provided training on cybercrime and electronic evidence for judges and prosecutors, in collaboration with the CoE under GLACY+ project.
  - NCA has established a CERT which forms part of the investigative branch of NCA. Primary mission: provide incident handling services for its internal constituents and to facilitate incident coordination, information exchange and analysis to look for trends and patterns in incident activity for its external constituents.
Recommendations:

3 – Developing a National Cybersecurity Strategy

Lessons on private sector cooperation and industry regulation

- **National Cybersecurity Strategy for South Africa**
  - Help to set out a vision, objectives, and priorities
  - Enables the govt 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 a cyber maturity assessment, priorities can be set based on empirical research results, allowing the country address real problems and promote trust in the online environment, in addition to improve cybersecurity awareness of the general public
Recommendations:
3 – Developing a National Cybersecurity Strategy

Lessons on private sector cooperation and industry regulation

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.
Recommendations: 4 – Cyber Capacity

Lessons on private sector cooperation and industry regulation

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

In brief, we recommend the following actions for ICASA:

- 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.

- 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.

- Based on the findings from the CMA, support the implementation of a capacity building programme for public officials, along with national cyber hygiene interventions and awareness campaigns 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.