REPUBLIC OF NAMIBIA
Internet Governance and Cybersecurity in Namibia

Ms Elizabeth Ujarura Kamutuezu
Deputy Director : Ministry of ICT
Republic of Namibia,

IEEE ETAP Forum

30 May 2017
Background

- Namibia became Independent on the 21st March 1990 from South African colonial regime.
- The country total space is 824,000sq km and Windhoek is the capital city.
- The total population is 2.1 million while female population is 50.7% and majority of the population resides in rural areas.
- Namibia is sharing borders with South Africa, Angola, Zambia, Botswana and Zimbabwe.
- Namibia has eleven tribes and English is the official language while Afrikaans is also spoken by majority.
Introduction

It is evident that Internet is most connected and least protected and the expansion of cyberspace becomes salience feature of our daily life. Namibia enjoys over 100% mobile phone penetration; about 72.12% access to internet and 53% population has access to broadband. Cybersecurity plays a pivotal role in the continuing development of information technology and Internet services. In order to safeguard Namibia’s security and economic wellbeing, it is vital that the Country enhance cyber security and to protect information infrastructure and equally important is ensuring that the Internet is safe and that the growing numbers of Internet users are protected. This call for government intervention to develop appropriate legal responses as a result the Namibian government has drafted Electronic Transaction and Cybercrime Bill to address problems pertaining to safety and security of digital communications of any mode.
Namibia has a sound ICT legal framework that facilitate investment in the ICT sector. After independence since 1990, Namibia developed a series of laws and policies that aimed at promoting ICT in Namibia and these are:

1. Namibian Communications Act, 2009
2. Overarching ICT Policy, 2009
3. Telecommunications Policy,
5. Postal Policy and New Licensing Framework
6. Universal Access Policy
7. Digital Terrestrial Television Policy Guidelines
Namibia ICT at Glance

- West Africa Cable System (WACS) connectivity in 2011 and in 2012 Telecom Namibia (100% state owned company) inaugurated the West Africa Cable System (WACS) submarine cable that links 14 countries (International);
- 143 Post Offices countrywide;
- Telecom Namibia has laid about 7755 Km fiber optic cable across the country;
- The Ministry of ICT has established 26 Multi-Sectoral Community Centres (MSCC) across the country;
- There are 342 FM radio transmitters, 57 TV transmitters and 36 studios;
- Telecom Namibia has established 193 base stations / PoPs for Broadband coverage;
- MTC has established 661 active base stations / PoPs for Voice and Data connections, of which 221 are providing broadband (>1mbps) data services;
- Direct Marine Cable Connectivity: SAT-3; WACS; SEACOM; 4 International PoPs;
- National Backbone Network: 100% Digital; 9,025 km fibre; 295 PoPs; 228 Digital Destinations; 178 Towers;
- There are four Telecoms Operators: GSM-Based; 2 x Mobile, 2 x Fixed;
- There are six Internet Service Providers;
- The National IXP was commissioned in 2014;
- Broadband Access: 3G and 4G/ LTE networks;
- Access and Penetration: 7% fixed line; +120% mobile and 13% Internet;
- On the 17 June, 2015 The Namibia Broadcasting Corporation NBC (parastatal) has migrated from Analogue Television Broadcasting to Digital Terrestrial Television (DTT) broadcasting;
- DTT Migration: +70% DTT population coverage
IGF Objectives

- Serves as a forum for multistakeholders policy dialogue to discuss public policy issues related to key elements of Internet governance
- Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet
- Support international and regional coordination and collaboration
- Discuss, inter alia, issues relating to critical Internet resources;
- Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.
IGF Benefits

- Free flow of ideas, knowledge and information over the internet-It allows participants to discuss freely, to voice their opinions, to think aloud, to think out of the box.
- Resolve issues related to security of user or network
- Establish standards of exchange of information to avoid piracy
- Developing methods to keep personal and confidential data secrecy
- Explore methods and policies for better internet performance and governance
Stakeholders

Anyone who has a stake in the future of the Internet
Working Committee

- Multi-Stakeholder Coordinating Team
- Disseminate all relevant information pertaining to NamIGF to all relevant stakeholders through the NamIGF website and emailing list
- Collaborate with partners to mobilise resources to support the Nam IGF programme
- Organise NamIGF every year
Defining Cyber Crime

Cyber Crime - any criminal act dealing with computers and networks, where the computer is a tool, target, or both
Types of Offences

- Offences against confidentiality, integrity and availability of computer Data and Systems
  - Illegal access (hacking) – unlawful access to a computer system.
  - Illegal data acquisition (data espionage) – internet used to obtain trade secrets/personal information such as bank account or credit card numbers.
  - Illegal Interception: offenders can intercept communications between users to record information exchanged.
  - Data interference: users depend on the availability of data and interference can result in financial losses.

- Content related offences
  - This category covers content that is considered illegal such as child pornography and xenophobic material, libel and false information, spam, copyright and related offences, trademark related offences etc.
Types of Offences

Computer related offences

- Computer-related Fraud: it enables the offender to use automation and software tools to mask criminals identities.
- Computer related forgery: refers to the manipulation of digital documents e.g. Altering text documents.
- Phishing: acts that are carried out to make victims disclose personal information.
- Misuse of devices: specially designed software tools used to attack other computers.

Combination offences

This category covers various terms used to describe complex scams that combine a number of different offences. For example: phishing and cyber laundering.
Drivers of Cybercrime

- Weak technology
- Vulnerable/unauthorised software
- Limited accountability
- Inconsistent and incomplete legislation/regulations
- Difficulty tracking and prosecuting criminals
- Limited jurisdiction
- Uninformed, misguided and malicious users - weak passwords, divulging passwords, opening unknown emails
Who are Cyber Criminals?

- Hackers
- Malicious insiders
- Industrial espionage
- Bored, disgruntled, or overburdened employees
- Naïve/uninformed computer users
- Organized crime
- Terrorists
- Paedophiles and molesters
- Petty criminals
- Foreign governments
Achievements

- Established NIGF Working Committee
- NIGF will be hosted in October 2017
- In process of Establishing CIRT
- Electronic Transaction and cybercrime Bill under public consultation
Challenges

- The IGF is not a decision-making body
- Cybercrime is borderless
- The common challenges are Lack of a legal and regulatory framework to ensure cyber security
- There is lack of information, statistics and records of cybercrime committed in Namibia due to absence of laws, lack of capacity and general awareness of cybercrime.
Challenges

- Lack of public private institutional collaboration
- Low technical capacity and human capacity IT skills. Systems poorly designed and poorly managed
- Social networking is on the rise and increasingly cybercrimes are perpetrated through the social networks (Facebook, twitter etc.)
What can be done

- Public Advocacy / Awareness
- Conducive legal environment
- Institutional Capacity Building
- Harmonisation of laws (National and International)
Conclusion

- The government needs to work closely with the corporate entities; private sector to ensure the effective implementation cyber security strategy laws once is enacted.
- The private sector is a key stakeholder to combat cybercrime, since they supply most of the relevant technology, operates most of the systems and networks. The private operators are also victims of cybercrime and some attacks can lead to massive financial loss that will negatively affect the economy.

- Balancing Security vs Privacy
Thank You