CYBER SECURITY POLICY AND LEGAL FRAMEWORK FROM A SOUTH AFRICAN PERSPECTIVE

Presented by:

**Hon:** Mr. Obed Bapela, MP
Deputy Minister of Communications

at: Summit on Information and Network Security for Emerging Markets

21 September 2011
Preamble

The world has embraced technology and society and our people are more reliant on the use of communication technology.

Technology has brought a better way of doing things, in particular Internet and Mobile Phones.

In Africa where telephone density was low at 1 x phone per 100 people access, with mobile it is now at 600 Million mobile phones out of a population of 1 x billion.

Smart phones are increasing access to internet and with that to deal our people on the continent, access services such as e.g. m-Health, e-Education, Telemedicine's, m-Agriculture, M-Money (M-pesa), with millions people unbanked now using mobile to send and receive money,
Preamble

Smart phones are increasing access to internet and with that to deal our people on the continent, access services such as e.g. m-Health, e-Education, Telemedicine's, m-Agriculture, M-Money (M-pesa), with millions people unbanked now using mobile to send and receive money, but with all this good developments comes new challenges such as threats of cyber security and the common one’s are: phishing, impersonating, hacking, (but for some reasons< the network infrastructure is not under attack even in countries with conflicts, e.g. Somalia, Libya, DRC and Cote I’voire, etc).
Preamble

Concurring with other speakers yesterday about the world that will face two new challenges,
1. Natural disaster,
2. Man made disaster such as the phenomena of cyber security.

Agreeing that while each country is facing different challenges of cyber and their priorities will be dictated to by their own immediate challenges.

However agree that we need Global solutions that are guidelines with common standards with can be adopted locally.

Cyber crime / cyber security and security networks is the new agenda that seeks new solutions.
Preamble

① In Africa with access and penetration on mobile and increase in internet access, will need to start with discussions to find solutions to counter cyber security/ cyber crime while at the same time building confidence and trust on the use of communication technology.

② The three countries that are already targets in Africa are; South Africa, Nigeria and Egypt because they are Middle Income Economies and attacks are on phishing in financial markets, certain targetted individuals or ignorant innocent people.

③ We have hackers who will do it for fun, and attack the networks, and isolated incidents on economic sabotage.
South African context on Cybersecurity

In the South African context, cybersecurity encompasses:

1. Cybersecurity matters impacting on national security;
2. Interventions and strategies for Combating Cybercrime; and
3. The need to build confidence and trust in pursuit to WSIS objectives.
Cybersecurity environment in South Africa

The cybersecurity environment in South Africa is characterized by:

- Policies and legislation that govern and regulate various aspects of cybersecurity.
- Institutional structures such as ICASA (national regulator); Films and Publication Board etc.
- Industry which plays a big role in ensuring that our information and network security is constantly appraised.
Policy and Legal framework

In South Africa, a number of legislation have bearing on cybersecurity, such as:

1. National Convention Arms Control Act (Act 41 of 2002);
2. Electronic Communications and Transactions Act (Act 25 of 2002);
Policy and legal framework

1. Regulation of Interception of Communications and Provision of Communications Related Information Act (Act 70 of 2002): Interception is for purpose of law enforcement and gathering of intelligence


3. Conventional Arms Control Regulations (R7969 of 2004)

4. Cryptographic regulations (R 8418, of 2006)
RICA and ECT Act

For purposes of my presentation today, I will focus on aspects of the South African legislation that my Department is directly responsible for:

1. *Regulation of Interception of Communications and Provision of Communications Related Information Act.*

In terms of the RICA Act, the Minister of Communications is responsible for:

- Issuing directives to determine manner in which electronic communication service providers must make their systems interceptable and store information;
- prescribing technical, security and functional requirements of interception facilities and devices;
Status of RICA implementation

- With the support of electronic communication service providers, South Africa has a database of all mobile subscribers' physical addresses.
- Database of 50 million registered subscribers (telemetry, data, voice).
Electronic and Communications Act (ECT Act)

On matters related to cybersecurity, the ECT Act provides for the following:

- Facilitating electronic Transactions;
- Cryptography Services;
- Authentication services providers;
- Consumer Protection;
- Protection of personal Information;
- Protection of critical databases;
- Domain Name Authority and Administration; and
- Establishment of a Cyber inspectorate.
Facilitating Electronic Transactions

Provides for the removal of social and legal barriers to electronic transacting. To this end, it provides for the legal recognition to data messages and records. Provision is made for the legal recognition of electronic signatures and “advanced electronic signatures” – a secure form of electronic signing.

It also deals with the rights and obligations that follow from the communication of data messages, namely contract formation. The time and place of sending and receiving data messages, as well as the time and place where a contract is deemed to be formed by means of data messages are provided for. The Act also provides for the validity of sending notices and other declarations of intent through data messages.

Currently being reviewed, especially on matters regarding electronic evidence.
Cryptography Services

This clause creates a regulatory framework for Cryptography products and services used in the Country. It provides for the establishment and maintenance of a Cryptography Provider Register by the Department of Communications. The objective is to assist law enforcement in their investigations; and this compliments the of RICA Act.
Electronic and Communications Act (ECT Act)

Authentication Service Providers
Provides for the establishment of an Accreditation Authority, that will accredit authentication products and service and will also monitor compliance to ensure that there is adherence by the accredited service providers.

The South African Accreditation Authority is currently evaluating an application for accreditation and a second application is due in Oct-Nov 2011. This will contribute to secure online communication.
Electronic and Communications Act (ECT Act)

Consumer Protection:

- Deals with consumer rights and issues pertaining to electronic transactions, provides for information, which must be made available to consumers before the conclusion of an on-line transaction, “cooling off” period within which they may cancel transactions concluded on-line without incurring any penalty. Consumers also have the right not to be bound to unsolicited communications offering goods or services. The Act also places the responsibility on businesses trading on-line to make use of sufficiently secure payment systems.

- This provision has been superseded by the Consumer Protection Act. A Consumer Protection Commission has been established to ensure online and offline consumers are not ripped off.

- ECT Act in the process of being aligned to this legislation.
Protection of personal Information

- Provides for the protection of personal information; regulates the collection of personal information through electronic transactions or electronic communications and grants the necessary authority to the Department to enforce the provisions of this clause of the Act.

- This provision will soon be superseded by the Protection of Personal Information (PPI) Act, which is currently a Bill being discussed in Parliament.
Electronic and Communications Act (ECT Act)

Protection of critical databases;

- Provides for the Minister of Communications to prescribe minimum standards on how to manage and maintain critical databases.

- Whilst this matter is partly addressed in the Protection of Personal Information Bill, it has become imperative that we not only protect critical databases but we protect critical information infrastructure. The Cybersecurity policy currently being finalised will address this shortcoming.
Establishment of a Cyber Inspectorate

The Act provided for the establishment of the Cyber Inspectorate to enforce provision off the ECT Act. We have not yet succeeded in the establishment of the Cyber Inspectorate, however a process is underway.

Based on developments in the field of cybersecurity, the role of the Cyber Inspectorate will have to be extended beyond the scope of the current ECT Act.
Draft National Cybersecurity Policy Framework

Notwithstanding the policy and legislation put in place in South Africa, our dependence on ICT’s for most aspects of our lives has necessitated the development of a National Cybersecurity Policy Framework.
Purpose of NCPF is to create:

- a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and understanding of cybersecurity in support of national security imperatives and the economy.

- The development of an information society which takes into account the fundamental rights of every South African citizen to privacy, security, dignity, access to information, the right to communication and freedom of expression.
NCPF Objectives

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;

Anticipate and confront emerging cyber threats and coordinate responses thereto.

Foster cooperation and coordination between Government, the private sector and civil society.
CYBERSECURITY OBJECTIVES continue

③ Promote international cooperation;

④ Develop requisite skills, research and development capacity;

⑤ Promote a culture of cybersecurity; and

⑥ Promote compliance with appropriate technical and operational Cybersecurity standards.
Conclusion

As a developing country, information and network security must be understood and viewed within a broader context of cybersecurity. The standard of information and network security in South Africa does meet global business expectation. We view information and network security as a critical element as we further expand on broadband network and advance in the attainment of the WSIS objectives.
THANK YOU