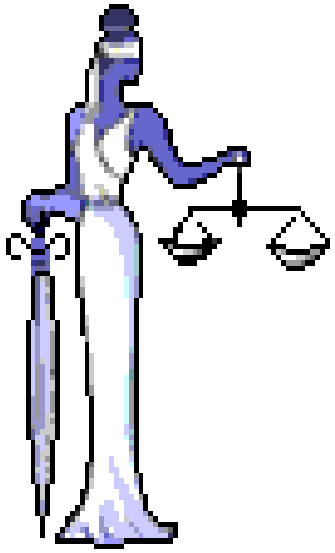
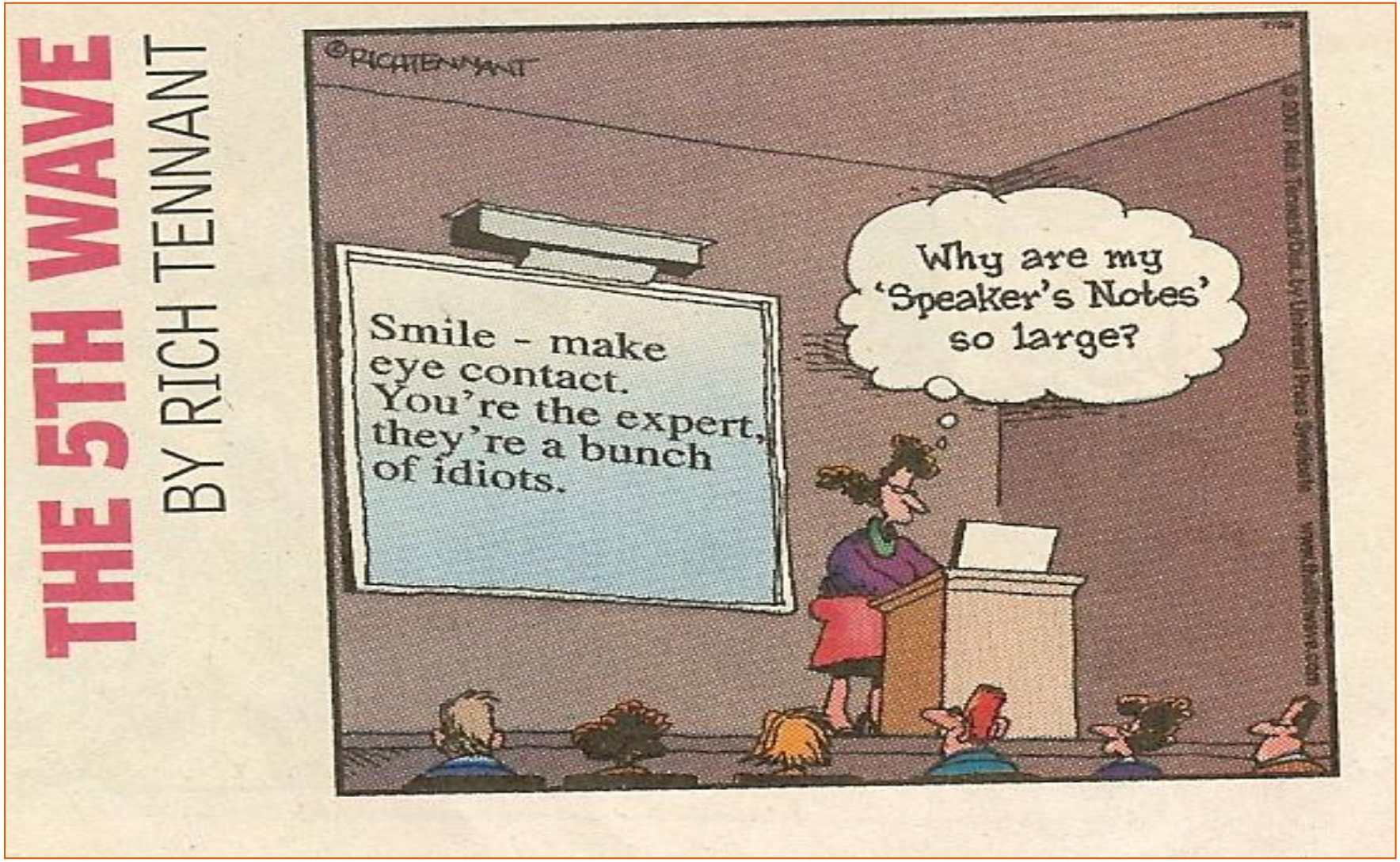
A SOUTH AFRICAN LEGAL PERSPECTIVE ON STATE GOVERNANCE OF CYBER SECURITY WITHIN AN AFRICAN AND GLOBAL CONTEXT



MURDOCH WATNEY

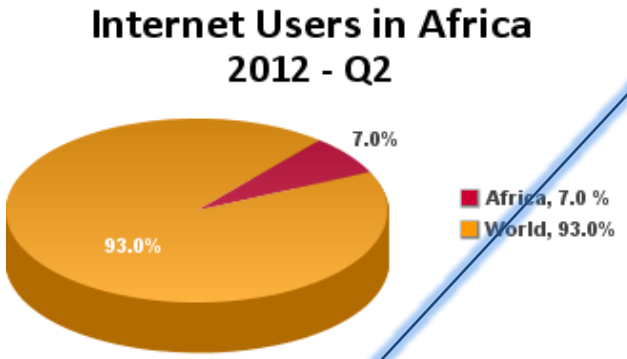
UNIVERSITY OF JOHANNESBURG

A Legal Perspective on State Governance of Cyber Security within an African and Global context

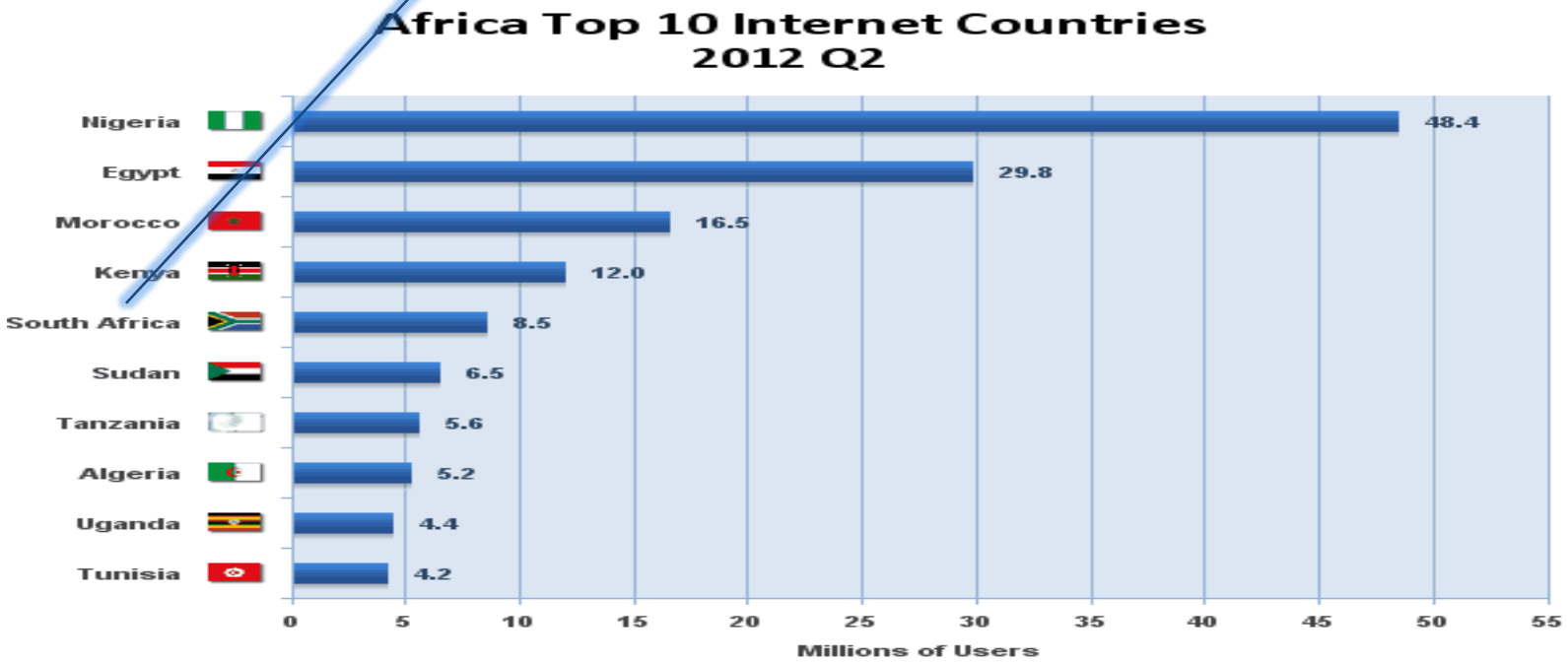


Statistics regarding Internet use and penetration

South Africa within the African continent regarding connectivity and benefiting from access to the Internet, for example economically but also ICT applications such as e-government, e-education, e-health



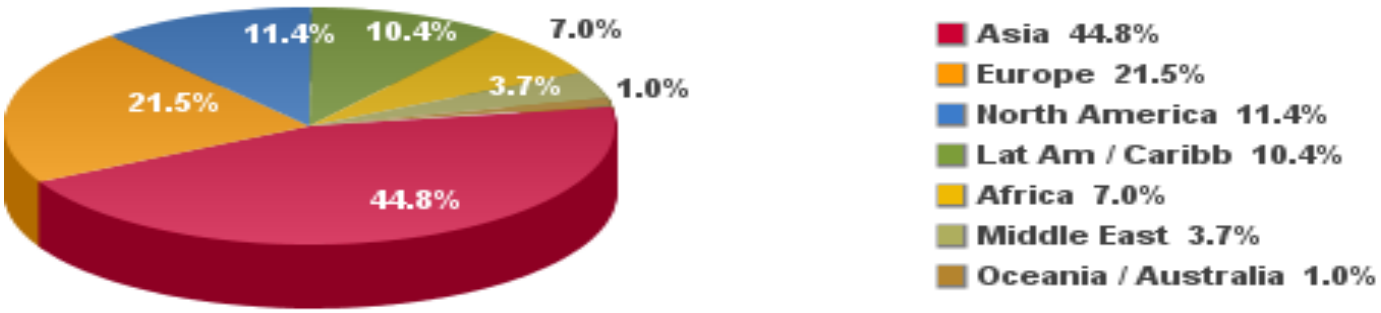
SA: technology not sufficient in providing access to ICT; e.g. broadband – wireless broadband : radio spectrum reallocation; and bandwidth: broadcasting migration: terrestrial television from analogue to digital broadcasting technology.



Source: Internet World Stats - www.internetworldstats.com/stats1.htm
167,335,676 Internet Users in Africa estimated for June 30, 2012

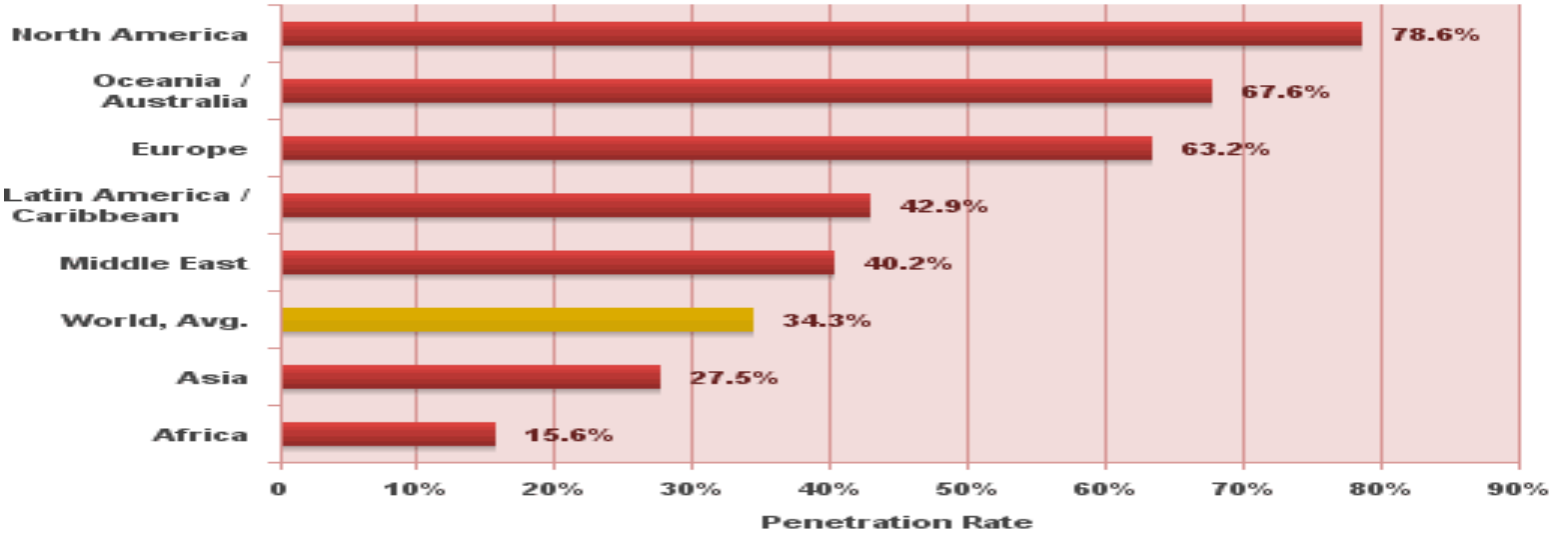
Statistics of interne use and penetration

Internet Users in the World
Distribution by World Regions - 2012 Q2



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 2,405,518,376 Internet users on June 30, 2012

World Internet Penetration Rates
by Geographic Regions - 2012 Q2



Source: Internet World Stats - www.internetworldststs.com/stats.htm
Penetration Rates are based on a world population of 7,017,846,922 and 2,405,518,376 estimated Internet users on June 30, 2012.

AN OUTLINE OF THE ASPECTS THAT WILL BE DISCUSSED REGARDING THE TOPIC, A SOUTH AFRICAN LEGAL PERSPECTIVE ON STATE GOVERNANCE OF CYBERSECURITY WITHIN AN AFRICAN AND GLOBAL CONTEXT:

The following aspects will be discussed:

i. An introduction to the topic;

ii. Definitions of cyber security related concepts;

The introduction and definitions serve as background to:

iii. An overview of the South African National Cyber Security Policy Framework (NCPF);

iv. The effect of global and international regulation of cyber security on the South African National Cyber Security Policy Framework (NCPF); and

v. Conclusion.

1. INTRODUCTION

Question: Why did I decide on the topic, namely a SA legal perspective on state governance of cyber security?

Answer:

i. On a national and global level there have been an on-going discussion on what should be done to ensure the cyber environment is protected against crime and once the security has been breached, how it should be investigated.

- The answer lies with cyber security.
  - In 2012 at the International Telecommunications Union (ITU) World Conference on International Telecommunications (WCIT – 12) it was correctly stated that cyber security is used increasingly as a catchword but it has many meanings depending of the context within which it is used.
  - Cyber security will be discussed within the context of the South African National Cyber Security Policy Framework (NCPF) which was approved by the cabinet in 2012.
    - The discussion is from a LEGAL PERSPECTIVE.

1.INTRODUCTION (continues)

ii. In 2012 Michael Moran, acting assistant director of cyber security and cybercrime at Interpol, stated at a conference: "We need better laws to deal with cybercrime".

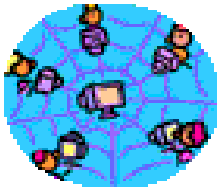
- Who are the 'we' that need to make better laws?
  - Within a global internet-connected world this question is important.
    - To tie in with the theme of the conference: Which role does the African continent play?
  - It is even more relevant after the ITU WCIT – 12.
- What will make the present laws better?
  - Nationally: each Internet connected nation-state must have national laws in place that are enforceable.
  - Globally and internationally?

iii. The topic touches on aspects that may look unrelated to cyber security.

- For example Africa (specifically southern) Africa's internet connectivity, access and penetration, the impact of discussions at the WCIT – 12 on Africa.

- The down side to this topic is that it has the potential to be a theoretical discussion.
  - One must look at the topic within a practical context;.
  - How does cyber environment look on a national and global level? For example most fraud within a commercial environment in SA is committed electronically; all prosecutors report on cyber crime statistics to the NPA; therefore question is: how can cyber security be used to prevent this crime and if breached, is the criminal justice system effective?

2.DEFINING CYBER SECURITY RELATED CONCEPTS



- There exists no universal definition of concepts.
  - Definitions are open to criticism;
  - Definitions serve as a point of reference.
- Cyber security is defined in the NCPF as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organisation and user assets.
  - How does the concept, cyber security differ from the concept, information security?
- The definition of cyber security must be seen within a specific context, namely the cyber security legal policy framework as envisaged by the NCFP which encompasses technical and non-technical matters.
- <u>The aim of cyber security within the ambit of the NCPF is to protect :</u>

  <u>i. the internet, cyberspace and ICTs</u>
  - A distinction should be drawn between the internet and cyberspace since this distinction may be relevant regarding regulation.

<u>against ii. cyber risks or threats</u>

2.DEFINING CYBER SECURITY RELATED CONCEPTS (continues)

- Cyber threat or cyber risk is an umbrella term that includes cyber crime and cyber intelligence crimes.

- Cyber security is not the same as cyber crime, but definitely inter-linked.
  - For example the following statement was made: "As the world is fast becoming one big digital globe, cyber security threatens to undermine this envisaged man-made wonder to simplify life in a way too complex to imagine."
- Which approach on national level may be used to regulate cyber security?
  - Distinguish between different models:
    - A state governance model including multi-stakeholders (top to bottom governance which includes private sector involvement);
      - ✓ Explains the title of the discussion.
    - A private sector driven model which includes the government but as an equal partner (bottom to top governance); and
    - A strict regulatory governmental control approach (top to bottom control in a prescriptive manner).

3. A BRIEF OVERVIEW OF THE SOUTH AFRICAN NATIONAL CYBERSECURITY POLICY FRAMEWORK (NCPF)

- The NCPF was developed by the Justice, Crime Prevention and Security (JCPS) Cluster that will be responsible for the implementation of the NCPF with the assistance of other government departments.
- The main purpose of the NCPF is providing a legal framework to ensure an aligned and coordinated approach to cyber security.
- The purpose will be achieved by the following policy positions:
  a. Address national security threats in terms of cyberspace;
  b. Combat cyber warfare, cyber crime and cyber ills;
  c. Develop, review and update existing substantive and procedural laws to ensure alignment; and
  d. Build confidence and trust in the secure use of ICTs.
- Cyber threats poses a risk to law enforcement and national security agencies.
  - The approaches to and purpose of crime prevention, detection, investigation and prosecution will be different.
  - Different interests are protected, e.g.
    - National security protection against cyber warfare, cyber espionage, cyber terrorism that may threaten the critical infrastructure.
    - Law enforcement protection would be protecting a company against espionage for commercial purpose, hacking etc.
- Different government departments will be involved with cyber security issues and responsible for different cyber security aspects:

➢ Department of Justice and Constitutional Development and National Prosecuting Authority will be responsible for:

- Facilitating cybercrime prosecution and court processes in accordance with laws; and
- Aligning all laws to ensure a coherent and integrated cybercrime prosecution approach in SA.

Overview of NCPF

- Department of SA Police Service:
  - Responsible for crime prevention and investigation;
  - Must also develop cross-border law enforcement cooperation; and
  - Promote international cooperation to fight cybercrime.
- Department of Communications will be responsible for:
  - Training of cyber security inspectors provided for in chapter 12 of the ECT Act
  - National Cyber Security Advisory Council (NCAC)
    - Advice the Minister of Communications on policy and matters relating to cyberlaw.
  - National Cyber Security Incident Response Team (CSIRT)
    - CSIRT will act as a single point of contact;
    - Establish information-sharing processes and procedures with the NCCC; and
    - All stakeholders involved (not only a government focused CSIRT)
- Department of State Security will be responsible for:
  - National Cyber Security Coordinating Centre (NCCC)
    - Key focus will be on national cyber security such as protecting the national cyber security critical infrastructure (many of the infrastructure in the hands of private companies) against cyber warfare, espionage, terrorism;
    - All National Critical Information Infrastructure (NCII) must be identified;
    - Developing a NCII strategy that will address the identification and protection of NCII by
    - Developing NCII regulations such as information security policy and procedures;
    - Facilitating an effective business –government partnership in implementation of the NCII Protection plan (many NCII privately owned for commercial purposes).
    - Will play an oversight and coordinating role in the national Cyber security Incident Response team (CSIRT).
- Any comment in respect of the NCPF?

4.THE EFFECT OF AFRICAN, MULTI-NATIONAL AND INTERNATIONAL CYBERSECURITY REGULATION ON THE SOUTH AFRICAN NATIONAL CYBER SECURITY POLICY FRAMEWORK.

4.1 Introduction

- A nation state without national cyber security laws or with national laws that are not enforced and/or a continent without cyber security will constitute a weak link.
  - Some may argue that in cyberspace a person is a 'netizen', a so-called citizen of the internet but from a legal perspective a person accesses the internet in a physical place and crime will have an origin and effect.
    - Barlow in 1996 posted "A declaration of the Independence of Cyberspace" on the Internet. In the Declaration he stated that there exists no elected government in cyberspace, that the governments have no sovereignty in cyberspace and "nor do you possess any methods of enforcement we have true reason to fear." In the Declaration of Independence he stated that although government may indicate that there exist problems that should be addressed, these problems will be addressed by the internet society themselves. He stated in the Declaration "(w)e will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before."
    - Is the Internet society above crime commission? First worm, Morris worm in 1988 and 'I love you' virus in 2000
- Cyber threats are borderless (multi-jurisdictional) and therefore it is well acknowledged that national laws alone will not be sufficient but on a global level there should also be cooperation between states in respect of cyber security breaches/cyber crime.
- Above achieved by means of harmonised laws on national level.

4.2.1 Southern Africa's Development Community (SADC) Model Law on Computer Crime and Cybercrime

- SADC, a regional community, consists of 15 member states, namely South Africa, Namibia, Botswana, Mozambique, Angola, Zimbabwe, Zambia, Democratic Republic of Congo, United Republic of Tanzania, Malawi, Mauritius, Madagascar, Seychelles, Kingdom of Swaziland and Lesotho.
- The ITU is assisting SADC in establishing a Model Law on Computer Crime and Cybercrime.
  - The project is referred to as the Support for Harmonisation of ICT Policies in Sub-Sahara Africa (HIPSSA): SADC Harmonised Legal Cyber Security Framework for Southern Africa.
  - It is under leadership of Prof Gercke who for the ITU Telecommunications Development compiled in 2011 a report "Understanding cybercrime: A Guide for Developing Countries."
- It has been stated that 4 of the 15 SADC member states have cybercrime legislation in place, namely South Africa, Botswana, Mauritius and Zambia.
- The Draft Model Law consists of 6 parts: part 1: preliminary; part 2: offences; part 3: jurisdiction; part 4: electronic evidence; part 5: procedural law and part vi: liability of providers.

4.2.3 African Union (AU) Draft Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.

- The AU consists of 54 states (excluding Morocco).
- The different AU member states have their own cultural, economic and political views which will affect the model implemented to regulate cyber security.
  - The latter is important to keep in mind when looking at the Council of Europe Convention on Cybercrime at par. 4.3 hereafter.
  - On a national level AU member states will implement their own model of state security.
- The AU Commission in conjunction with the UN Economic Commission for Africa (UNECA) is busy drafting a AU Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.
  - It covers 4 key areas, namely part 1: e-transactions; part 2: personal data protection; part 3 cybercrime and cyber security.
- Comments on the Draft AU Convention.
  - The part dealing with cybercrime and cyber security was drafted in language that does not read easily .
  - It is drafted in vague language but understandable as countries have different procedural models: SA has an adversarial/accusatorial procedural model whereas other countries have an inquisitorial model. It does for example refer to the principle of double criminality.
  - **Most importantly, it is a starting point in ensuring the African continent has cyber security/cybercrime legislation in place, it ensures that Africa does not become a haven for cyber criminals.**

4.3 The global effect of the Council of Europe (CoE) Convention on Cybercrime

- The Budapest Cybercrime Convention is not an international convention but a multi-national convention.
  - It was signed in 2001 in Budapest, Hungary.
  - Out of the 30 countries that signed it, 4 were non-European countries, namely SA, USA, Japan and Canada.
- The Cybercrime Convention is commendable.
  - It provides for substantive and procedural measures to combat, investigate and prosecute cybercrime aimed at harmonisation of laws and co-operation and assistance in crime commission.
- Only 39 countries have ratified the Cybercrime Convention.
  - For example Russia and China have not signed/ratified it.
- Will the CoE Cybercrime Convention become a global cybercrime treaty?

4.4 United Nations in respect of legal regulation of cyber security.

- As indicated, there is no international treaty on cybercrime.
- There has been calls for an international treaty on cybercrime.
  - The USA is of the opinion that there is no need for an international body or treaty but regulation can be achieved between countries by means of multi-national treaties.
  - China and Russia wants an international body to regulate cyber crime.
- The question so far has been whether the international law is effective enough in case of cyberwar.
  - NATO for example stated that in their opinion international law is at present sufficient to cover cyberwar but it depends on interpretation.
  - Article 51 of the UN Charter provides for self-defense against an 'armed attack.'
    - May a cyber attack be considered an 'armed attack' in terms of 'conventional' international law?
      - ❑ Debatable whether cyber attack is an 'armed attack.'
      - ❑ Would Estonia have been able to launch a counter attack?
    - However, the position may be different if the attack launched against a nation state is destructive?
      - ❑ E.g. A virus or malicious software may disable electronic power systems or hi-jack air traffic control systems.
    - Even if it is an act of war, how may a nation-state retaliate in self-defense?
      - ❑ International law of war is based on the principle of proportionality.

        E.g. If Estonia launched a counter offensive: may it bomb Russia or attack the computers used as 'botnets' in other countries that were unaware the computer was being used as a 'botnet'?

4.4 United Nations in respect of legal regulation of cyber security (continues)

- In 2011 China, the Russian Federation, Tajikistan and Uzbekistan requested the United Nations for an international code of conduct for information security.
  - Nation-states would voluntarily subscribe to it and pledge for example:
    - Not to use ICTs to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies;
    - To cooperate in combatting criminal and terrorist activities;
    - To reaffirm the rights and responsibilities of States to protect in accordance with relevance laws and regulations, their information space and critical information infrastructure;
    - To promote the establishment of a multilateral, transparent and democratic international internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet;
    - To assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide.

4.4 United Nations in respect of legal regulation of cyber security (continues)

- The International Telecommunications Union (ITU) World Conference on International Telecommunications (WCIT- 12) must be seen against the above given background.
  - The ITU is a specialized UN agency to promote the development, efficient operation and general availability of telecommunications facilities and services e.g. to develop technology for seamless connection between technology and networks, allocate satellite orbits and radio spectrums.
  - The purpose of the conference was to agree to updates to 1988 international telecommunications regulations.
  - Unfortunately the WCIT – 12 was used to finally confirm the tensions between western and non-western nation-states regarding international regulation and brought the conflict to the fore.
    - It was not the ideal forum to openly show the divide but in the absence of a forum it was inevitable.
  - The treaty updates was signed by 89 states of the 151 member states that attended the conference and will come in operation in 2015.
    - It was signed by so-called non-western countries which included African states, China and Russia.
  - The treaty was severely criticised by western countries.
    - In the preamble all member states have a right of access to international telecommunications services.
    - Article 5 of the Regulation provides for security and robustness of networks.
    - In a resolution stated all governments should have an equal role and responsibility for internet governance and for ensuring the stability, security.

5.THE WAY FORWARD FOR CYBER SECURITY WITHIN A GLOBAL CONTEXT.

- On a national level:
  - Need an aligned and coordinated approach to cyber security.
  - Each country is sovereign and must decide on the model of cyber security regulation.
  - Laws cannot be merely ‘paper law’; the mechanisms for enforcement must be in place.
- On an international level:
  - All nation-states will have to agree on the way cyber crime/cyber security will be regulated.
  - All nation-states will have to be seen as equal partners in cyber security regulation.
  - Crimes such as cyber warfare is a reality and way of dealing with it will have to be discussed on an international level.