“Cyber Crime and Cyber Security Legislation in Africa - with an emphasis on Cyber Terrorism and Cyber Warfare from a South African Perspective.“

ICIL : 2016
Pretoria , South Africa

Sizwe Lindelo Snail Ka Mtuze

Director- Snail Attorneys @ Law Inc.

International Co-Ordinator – African Centre for Cyberlaw and Cybercrime

Adjunct Research Fellow – Fort Hare University

SNAIL ATTORNEYS AT LAW

University of Fort Hare
Together in Excellence

CONCILIUM NOVI MUNDI
ECIPS

African Center for Cyberlaw and Cybercrime Prevention (ACCP)

TABLE OF CONTENTS

University of Fort Hare
Together in Excellence

African response to Cybercrime and Cyber Security

EAST AFRICAN COMMUNITY

SOUTHERN AFRICAN DEVELOPMENT COMMUNITY
TOWARDS A COMMON FUTURE

African Union
a United and Strong Africa

Economic Community of West African States (ECOWAS)

The Supplementary Act on Cyber Crime

DIRECTIVE CIDIR. 1/08/11 ON FIGHTING CYBER CRIMEWITHIN ECOWAS

In 2009 ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states

Focus more on ***Cyber Crime , Search and Procedure*** *and* ***Data Protection***

SADC E-COMMERCE and Cyber Crime
MODEL LAW

SOUTHERN AFRICAN DEVELOPMENT COMMUNITY
TOWARDS A COMMON FUTURE

* LEGAL RECOGNITION OF ELECTRONIC COMMUNICATIONS and LEGAL EFFECT OF ELECTRONIC COMMUNICATIONS

* TIME AND PLACE OF DISPATCH AND RECEIPT OF ELECTRONIC COMMUNICATIONS

* THE PROTECTION OF ONLINE CONSUMERS

* EVIDENTIARY ISSUES AND VALUES OF ELECTRONIC EVIDENCE

* CYBER CRIME – SUBSTANTIVE AND PROCEDURAL LAW

* INTERMEDIARIES

SNAIL
ATTORNEYS AT LAW

EAST AFRICAN COMMUNITY

EAC LEGAL FRAMEWORK FOR CYBERLAWS
EAC 1 and EAC 2

Legal Framework and Recommendations

Electronic transactions and Issues of validity

Electronic Evidence

Electronic signatures and authentication

Computer crime

*Substantive offences
*Criminal procedure

Cyber Security

Consumer protection

Data protection and privacy

University of Fort Hare
Together in Excellence

African Union
a United and Strong Africa

The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa

- First piece of African International Law which is binding on all African Countries which are part of the African Union

- Deals with Aspects of E-Commerce, Cyber Crime and Cyber Security as a whole.

The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa

- **Article III – 1 – 1: Laws against cyber crime**

Each Member State shall adopt such legislative measures as it deems effective to set up material criminal offenses as acts which affect the confidentiality, integrity, availability and survivability of ICT systems and related infrastructure networks; as well as effective procedural measures for the arrest and prosecution of offenders.

Member States shall take into account the approved language choice in international cyber crime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations where necessary.

- "**Article III – 1 – 5: Harmonization "**

Each Member State shall ensure that the legislative measures adopted in respect of substantive and procedural provisions on cyber crime reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures.

The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (cont.)

- **"Article III – 1 – 19: Harmonization"**

Each Member State shall ensure that the legislative measures adopted in respect of material and procedural provisions on cyber security reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures."

The convention differentiates and proposes amendment to existing law with regards to :

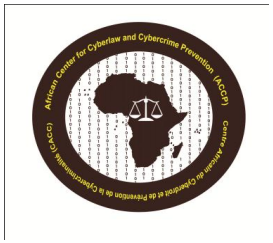
- Attack on computer systems
- Procedural Law
- Attack on computerized data
- Content related offenses
- Proposes adapting certain sanctions to the Information and Communication Technologies
- Offenses relating to electronic message security measures
- Offenses specific to Information and Communication Technologies
- Coporate liability
- Proposes adapting certain information and communication technologies offenses

The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (cont.)

<u>The Convention comes up with basic principles on Cyber Security :</u>

- ***National Cyber Security Monitoring structure.***
- ***Obligates all states to establish a National Cyber Security Framework***
- ***Encourages public-private partnership and International Co-operation***
- ***Obligates African states to adopt strategies & increase capacity building***
- ***Protection of Essential Information Infrastructure***

Obligates all African states to adopt strategies and increase capacity building



African Union
a United and Strong Africa

The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (cont.)

Further Basic principles on Cyber Security (cont):

- ***Establishment of Cyber Security System for all African States***
- ***Creation of National Computer Emergency Response Team (CERT)***
- ***Cross-boarder assistance relating to Cyber Security matters.***
- ***International Co-Operation of African States with other International states (outside the AU) to deal with Cyber Security threats***

CONCILIUM NOVI MUNDI
ECIPS

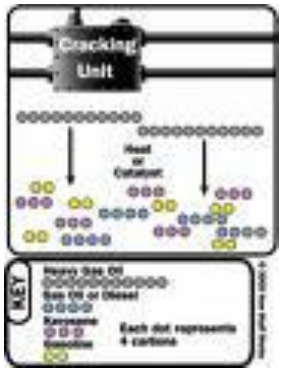
African Union
a United and Strong Africa

Cyber Crime and Cyber Security in South Africa

- **Section 85 defines 'unlawful access' as the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorized to access that data and still continues to access that data (S L. Geredal (2006) 282).**

- **Section 86(1) provides that, subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.**

Section 86(2) states that anyone who intentionally and without authority to do so interferes with data in a way which causes such data to be modified , destroyed or otherwise rendered ineffective is guilt of an offence.



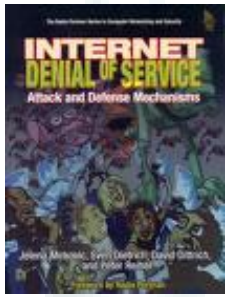
Section 86 (4) and 86(3) introduces a new form of crime known as the anti-cracking (or anti-thwarting) and hacking law. In terms of Section 86 (3) the provision and, or selling and, or designing and, or producing of anti-security circumventing (technology will be a punishable offence. (GJ Ebersoehn (2003) 16)

In terms of section 86(4) it is requirement to be guilt of this offence if the offender uses and designs a programme to overcome copyright protection, with direct intent to overcome a specific protection data protection programme (GJ Ebersoehn (2003) 17).

CONCILIUM NOVI MUNDI
ECIPS

Denial of service (DOS) attacks also popularly known as Disk Operating System attacks, are attacks that cause a computer system to be inaccessible to legitimate users.

Section 86(5) states that, "any person who commits any act described in **Section 86** with the intent to interfere with access to an information system so as to constitute a denial , including a partial denial of services to legitimate users is guilt of an offence ".



The act or conduct is fashioned in such a manner that it is widely defined and consist of any of the action criminalized in **Sections 86(1) – Section 86 (4).** The actions include unauthorized access, unauthorized modification or utilizing of a program or device to overcome security measures. (M Kufa (2008) 20)

SNAIL
ATTORNEYS AT LAW

Legal Aspects impacting on Law enforcement of Cyber crimes

(Procedural aspects of Cyber crimes)

Admissibility and Evidential Weight of data Messages (ECT Act S 15)

- After much legal uncertainly as to the admissibility of a printout in Court in terms of the Old Computer Evidence Act, Section 15 of the ECT, now states that the rules of evidence must not be used to deny admissibility of data messages on grounds that it's not in original form. A data message made in the ordinary course of business, or a printout correctly certified to be correct is admissible evidence. It constitutes rebuttable proof of its contents when it is produced in the form of a print-out.[1]

- The Act now states that Data messages shall be admissible giving due regard to reliability of manner of storage, generation and communication, reliability of admission manner of maintenance of message, manner in which originator is identified, and any other relevant factor. In other words the Act creates a rebuttable presumption of that data messages and or printouts thereof are admissible in evidence.[2]

[1] Also see the case of S B Jafta v Ezemvelo KZN Wildlife (Case D204/07) where a e-mail used to accept an employment contract was regarded as conclusive proof that the said employment had been accepted.

[2] also see the controversial case of S v Motata where electronic information (data in the form of images and sound) from cell phone was admitted into evidence in a trial within a trial (the case has yet to be concluded)

Regulation of Interception of Communications and Provision of Communication-related Information Act - RICA

The Interception and Monitoring Prohibition Act 127 of 1992 was repealed by the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (hereafter referred to as RICA).

RICA, the Electronic Communications Act 25 of 2002 and the Promotion of Access to Information Act 2 of 2000 (PROATIA) generally prohibit the unlawful interception or monitoring of any data message (Cohen 2001: 2–4).

RICA specifically governs the monitoring and/or interception of transmissions including e-mail. In Section 2 it states that:

" No person shall Intentionally intercept or attempt to intercept or authorize, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."

This is subject to the **"ground of justification "** in case of an emergency , serious criminal offence , necessity , if authorised by interception order and state security .

.

SNAIL
ATTORNEYS AT LAW

Regulation of Interception of Communications and Provision of Communication-related Information Act - RICA cont.

This means in simple terms that it is unlawful and therefore prohibited to:

1. **Intentionally and without the knowledge or permission of the dispatcher to intercept a communication** which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or

2. **Intentionally monitor any conversations or communications by means of a monitoring device** so as to gather confidential information concerning any person, body or organisation (Cohen 2001: 2–4).

- One must note that the attempt is as unlawful as the actual act of actually intercepting and monitoring a data communication

- Section 5(1) of RICA provides that any person may authorise or give anyone else ***"written"*** permission to monitor or intercept any data communication unless it is for the purposes of unlawful conduct.

  Modiba (2003: 366) suggests that if the employer in the workplace wants prior written consent to intercept and monitor communication devices at the workplace he should insist that the employee sign a document confirming such consent.

Other South African Laws and Cyber Security policies

- Cyber Inspectors in Terms of the ECT Act
- Monitoring and inspecting suspicious websites
- Investigate Cryptographers activities
- Audit critical database adminsitrators
- Carry out search and seizures
- ECS - CIRT
- Draft Cyber Security Policy

CONCILIUM NOVI MUNDI
ECIPS

Proposed Amendments- Cybercrimes and Related Matters Bill

Preamble of the Proposed BILL

- To create offences and impose penalties;
- to further regulate jurisdiction;
- to regulate the powers to investigate, search ,access or seize;
- to further regulate aspects of international cooperation in respect of the investigation of cybercrime;
- establishment of various structures to deal with cyber security;
- to regulate National Critical Information
- to further regulate aspects relating to evidence;
- to impose obligations on electronic communications service providers regarding aspects which may impact on cyber security;

University of Fort Hare
Together in Excellence

SNAIL
ATTORNEYS AT LAW

New Proposed Cyber Crime offences

- Section 2: Personal information related offences
- Section 3: Unlawful access
- Section 4: Unlawful interception of data
- Section 5: Unlawful acts in respect of hardware or software tools
- Section 6: Unlawful interference with data
- Section 7: Unlawful interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure
- Section 8: Unlawful acts in respect of malware
- Section 9: Unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices
- Section 10: Computer related fraud

New Proposed Cyber Crime offences

- Section 11: Computer related forgery and uttering
- Section 12: Computer related appropriation
- Section 13: Computer related extortion
- Section 14: Computer related terrorist activity and related offences
- Section 15: Computer related espionage and unlawful access to restricted data
- Section 16: Prohibition on dissemination of racist and xenophobic material
- Section 17: Prohibition on incitement of violence
- Section 18: Prohibited financial transactions
- Section 19: Infringement of copyright
- Section 20: Child pornography
- Section 21: Harbouring or concealing person who commit

SNAIL
ATTORNEYS AT LAW

Extended - **JURISDICTION clause**

The proposed Section 25 of the Bill

(1) A court in the Republic trying an offence in terms of this Act has jurisdiction where—

(*a*) the offence was committed in the Republic;
(*b*) any act or omission in preparation for the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;
(*c*) the offence was committed in the Republic or outside the Republic by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or
(*d*) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

(2) If the act or omission alleged to constitute an offence under this Act occurred outside the Republic, a court of the Republic, regardless of whether or not the act or omission constitutes an offence at the place of its commission, has jurisdiction in respect of that offence if the person to charged—

(*a*) is a citizen of the Republic;
(*b*) is ordinarily resident in the Republic;
(*c*) was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;
(*d*) is a company, incorporated or registered as such under any law, in the Republic; or
(*e*) any body of persons, corporate or unincorporated, in the Republic.

CONCILIUM NOVI MUNDI
ECIPS

Extended Jurisdiction clause cont.

(3) Any act or omission alleged to constitute an offence under this Act and which is committed outside the Republic by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act or omission constitutes an offence or not at the place of its commission, deemed to have also been committed in the Republic if that—

(*a*) act or omission affects or is intended to affect a public body, a business or any other person in the Republic;

(*b*) person is found to be in South Africa; and

(*c*) person is for one or other reason not extradited by South Africa or if there is no application to extradite that person.

(4) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person acted or, in case of an omission, should have acted.

University of Fort Hare
Together in Excellence

Proposed : POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE AND INTERNATIONAL COOPERATION

- Section 28: Search for and access to or seizure of, certain articles
- Section 29: Article to be accessed or seized under search warrant
- Section 30: Oral application for search warrant or amendment of warrant
- Section 31: Search and access or seizure without search warrant
- Section 32: Search and seizure for and access to article on arrest of person
- Section 33: Assisting member of law enforcement agency or investigator
- Section 34: Obstructing or hindering member of law enforcement agency or investigator who is accompanied by member of law enforcement agency and authority to overcome resistance
- Section 35: Powers conferred upon member of law enforcement agency or investigator who is accompanied by member of law enforcement agency to be conducted in decent and orderly manner with due regard to rights of other persons

Proposed: POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE AND INTERNATIONAL COOPERATION cont.

- Section 39: Expedited preservation of data direction
- Section 40: Disclosure of data direction
- Section 41: Preservation of evidence direction
- Section 42: Oral application for preservation of evidence direction
- Section 43: Access to data and receipt and forwarding of unsolicited information
- Section 44: Issuing of direction requesting foreign assistance and cooperation
- Section 45: Foreign requests for assistance and cooperation
- Section 46: Complying with order of designated judge
- Section 47: Informing foreign State of outcome of request for assistance and cooperation and furnishing of data to foreign State

SNAIL
ATTORNEYS AT LAW

New proposed clauses

EVIDENCE

- Section 59: Admissibility of affidavits
- Section 60: Admissibility of evidence obtained as result of direction requesting foreign assistance and cooperation
- Section 61: Admissibility of evidence

GENERAL OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND LIABILITY

- Section 62: General obligations of electronic communications service provider
- Section 63: Liability of electronic communications service provider

AGREEMENTS WITH FOREIGN STATE OR TERRITORY

- Section 64: President may enter into agreements

Further Proposed Clauses :

STRUCTURES TO DEAL WITH CYBER SECURITY

Section 49:	Cyber Response Committee
Section 50:	Cyber Security Centre
Section 51:	Government Security Incident Response Teams
Section 52:	National Cybercrime Centre
Section 53:	Cyber Command
Section 54:	Cyber Security Hub
Section 55:	Private Sector Security Incident Response Teams

University of Fort Hare
Together in Excellence

Further Proposed Clauses :

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Section 56: Identification and declaring National Critical Information Infrastructures

Section 57: Establishment and control of National Critical Information Infrastructure Fund

Section 58: Inspection of National Critical Information Infrastructures to ensure compliance

SNAIL
ATTORNEYS AT LAW

CONCILIUM NOVI MUNDI
ECIPS

African Center for Cyberlaw and Cybercrime Prevention (ACCP)
Centre Africain du Cyberdroit et de Prévention de la Cybercriminalité (CACC)

International Responses to Cyber Terrorism and Cyber warfare

- Draft International Convention to Enhance Protection from Cyber Crime and Terrorism

- Draft Convention proposes International Agency for Information Infrastructure Protection (IAIIP)
- Draft Convention proposes criminalisation of acts of Cyber crime linked to Cyber Terrorism
- Proposes definition for cyber terrorism :

  " Intentional use of or disruption of the cyber system (computer) or threat thereof of unlawful violence to further terrorist objectives such as , civil disorder and violence"

SNAIL
ATTORNEYS AT LAW

International Responses to Cyber Terrorism and Cyber warfare

- Cyber Terrorism divided into two categories namely “Effects based cyber terrorism” which concentrates of the effects of Cyber Terrorism
- “Intent based cyber terrorism” refers more to the use of the cyber system to plan and execute act of terror and recruitment and proliferation of terrorist material on e-mail and social media.
- “Cyber warfare” new battle field compared to the traditional war battlefield
- Difficult to regulate cyber warfare as it crosses jurisdiction and is not regulated

International Responses to Cyber Terrorism and Cyber warfare

- Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (cont)

- It is suggested that offenses against Cyber System and Critical infrastructure be created by states.
- Proposes criminalisation of hindrance of Cyber systems function done so intentionally and systematically
- Also suggest the crime of interfering with a cyber system with intent to do harm to the info or substantial damage
- It criminalises the misuse in particular the use to commits act of cyber terrorism using a cyber system
- It suggest prohibiting the use of cyber systems in act prohibited by international treaties (ie terrorism and cyber espionage)
- Other forms of malicious conduct targeted against a state and it inhabitants.

International Responses to Cyber Terrorism and Cyber warfare

- **Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (cont)**

- **Mutual national legal assistance is Key for successful prosecution**
- **Extradition of individual found committing cyber terrorism**
- **Draft Convention is not to be used for political means or objectives**
- **Cyber warfare defies traditional rules of engagement during war**
- **Cyber Warfare also introduces new concept of Cyber deterrence – which has its origins in the word "nuclear deterrence" which hinges on 3 (three) pillars :**

→ **Cyber resilience**

→ **Cyber Attribution**

→ **Developing cyber offensive and Cyber Defensive capabilities.**

CONCILIUM NOVI MUNDI
ECIPS

Concluding Remarks

Q & A

African Center for Cyberlaw and Cybercrime Prevention (ACCP)
Centre africain de Cyberlaw et de Prévention de la Cybercriminalité (CACC)

University of Fort Hare
Together in Excellence

SNAIL
ATTORNEYS AT LAW

Contact Us:

Attorney Sizwe LINDELO Snail ka Mtuze (LLB - UP) (LLM - UNISA)

Attorney and International Coordinator ACCP

E-mail : ssnail@Snailattorneys.com
www : www.snailattorneys.com
Tel / Fax : +27 (012) 757 8761
Fax : +27 (086) 617 5721
Cell : +27 (083) 477 4377