http://www.justice.gov.za/cfw/confw.htm

SPEECHES - 2013

Address by Mr Andries Nel, MP, Deputy Minister of Justice and Constitutional Development, at the Lex Informatica - 2013 Cyberlaw Conference: Advancement of cyberlaw and information ethics in Africa and globally held at the University of Pretoria on 4 April 2013

Program Director,
Organisers of the Conference and in particular Mr Sizwe Snail ka Mtuze,
Mr Coetzee Bester,
Prof Stephanie Burton, Vice-Principal (UP),
Distinguished Guests,
Honourable Delegates to and Speakers at the Conference, from both outside and inside South Africa,
Fellow South Africans,
Ladies and gentlemen

Thank you very much for inviting the Department of Justice and Constitutional Development to participate in this important and topical conference on the Advancement of Cyberlaw and Information Ethics in Africa and Globally.

I have been asked to contribute to this festival of ideas by contributing some perspectives on the Advancement of Cyberlaw in Africa and Globally and in doing so to share with you some of the steps being taken by the Justice, Crime Prevention and Security Cluster of Government to ensure a safe cyberspace for South Africa and our continent.

I would argue that nowhere is the correctness of South Africa's basic perspective to international relations demonstrated more clearly than in the domain of cyber-security.
Our fundamental strategic objective in the field of international relations is to ensure: A Better South Africa, in a Better Africa in a Better World.

Indeed the objective of a cyber-secure South Africa is inextricably linked to a cyber-secure Africa and a cyber-secure World.

Programme Director,
If anyone needed any convincing of this thesis it I would argue that is to be found in the fact that this conference takes place amidst what some have referred to as the biggest distributed denial of service attacks known to date.

According to yesterdays edition of the on-line newsletter Legalbrief eLaw and Management:

"A cyber-attack threatening to cripple the Internet has been traced to a Cold War command post in the Netherlands. Legalbrief reports that over the past two weeks it has affected regular data traffic mainly in Europe but also around the world. Spamhaus said the distributed denial of service (DDoS) attack started on relatively small scale on 19 March (a DDoS attack is carried out when the attacker sends so many requests to a server that it is overwhelmed and shuts down). The attack grew to the rate of 300bn bits per second of DDoS traffic - thatâ€™s about three times bigger than the biggest DDoS attacks known to date. The Guardian reports that the problem began when Spamhaus added a Dutch hosting organisation called Cyberbunker to its list of unwelcome Internet sites. The service has reportedly made 'plenty of enemies', and the cyber-attack appeared to be retaliation."

I am sure that the irony of cold war infrastructure designed for conventional warfare being used in a cyber attack will not be lost on the participants in this conference. Equally so, the fact that, as during the Cold War, the African Continent is again the subject of what in more recent times has come to be referred to by the un-euphemistic phrase: "collateral damage."

This conference also takes place little more than a week the conclusion of the highly successful Fifth BRICS Summit held in Durban. The theme of the summit was BRICS and Africa: Partnership for Development, Integration and Industrialisation.

Significantly, the eThekwini Declaration released at the conclusion of this historic summit and its accompanying Action plan and an agenda of new areas of cooperation that need to be explored before the next Summit, included the following statement on cyber-security:

"We recognize the critical positive role the Internet plays globally in promoting economic, social and cultural development. We believe itâ€™s important to contribute to and participate in a peaceful, secure, and open cyberspace and we emphasise that security in the use of Information and Communication Technologies (ICTs) through universally accepted norms, standards and practices is of paramount importance."
This statement, as well as the inclusion of cyber-security on the BRICS new agenda for exploration and cooperation, makes it clear that cyber-secrity is firmly on the BRICS agenda and regarded as integrals to promoting economic, social and cultural development.

Programme Director,
Cybersecurity is by its nature a global problem that requires international, regional and national solutions.

Unfortunately, there is not complete consensus on how to deal most effectively with these issues and it is clear that countries and power blocs, whether it be regionally or globally, have different approaches.

One of these instruments is the Budapest Convention on Cybercrime. Originally developed by the Council of Europe, it is an international instrument that serves as a guideline for developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties.

The convention has been ratified by 39 States, including the United States, Canada and Japan. A further 10 states, including South Africa, have signed but not ratified the Convention.

Whilst recognizing the important contribution made by the Budapest Convention a number of States have advanced the call for a more a universal international instrument.

The Salvador Declaration, adopted at the conclusion of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice during April 2010, in Brazil, called, for example, for a specific study to be conducted in respect of cybercrime with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

This recommendation was adopted by the UN Commission on Crime Prevention and Criminal Justice, the Economic and Social Council as well as the UN General Assembly.

The outcome of the study is expected later in 2013 or 2014 and should give us an indication whether there is a need for a new international instrument under the auspices of the United Nations.

During 2011, the permanent representatives of China, Russia, Tajikistan and Uzbekistan to the United Nations submitted a letter jointly to the United Nations Secretary-General Ban Ki-moon, asking him to distribute the International Code of Conduct for Information Security drafted by their countries as a formal document of the 66th session the General Assembly and called upon countries to further discuss the document within the framework of the United Nations so as to reach consensus on the international norms and rules standardizing the behavior of countries concerning information and cyberspace. Though this is work in progress the International Code of Conduct for Information Security raises a series of basic principles of maintaining information and network security which cover the political, military, economic, social, cultural, technical and other aspects. The principles stipulate that countries shall not use such information and telecom technologies as the network to conduct hostile behaviors and acts of aggression or to threaten international peace and security and stress that countries have the rights and obligations to protect their information and cyberspace as well as key information and network infrastructure from threats, interference and sabotage attacks. They also advocate establishing a multilateral, transparent and democratic international Internet governance mechanism, fully respecting the rights and freedom of information and cyberspace with the premise of observing laws, helping developing countries develop the information and network technologies and cooperating on fighting cybercrimes.

The ITU, originally founded as the International Telegraph Union, is a specialized agency of the United Nations responsible for issues that concern information and communication technologies.

In 2007 the ITU launched the Global Cyber-Security Agenda (GCA) as a framework for international cooperation aimed at enhancing confidence and security in the information society.

This in turn has led to the initiation of programmes such as the Child Online Protection. Through its partnership with the International Multilateral Partnership Against Cyber Threats (IMPACT) and with the support of leading global players, ITU is also currently deploying cybersecurity solutions to countries around the world. Part of this was the setting up of a Cyber-security Gateway whose purpose is to provide a user friendly interactive information resource on national and international cybersecurity related initiatives world-wide.

At the level of the Commonwealth specific templates or models were developed to assist with the development of domestic legislative provisions, such as the Commonwealth Model Law on Computer and Computer Related Crime (also called the Commonwealth Model Law), the London Scheme on Extradition and the recent revisions to the Scheme Relating to Mutual Assistance in Criminal Matters in the Commonwealth (called the Harare Scheme).

In addition, at the meeting of Commonwealth Law Ministers held in July 2011 in Sydney, Australia, Ministers recognised the significant threat posed by cybercrime to national security and law enforcement in all countries of the Commonwealth and mandated the Commonwealth Secretariat to establish "a multidisciplinary working group of experts to:

- review the practical implications of cybercrime in the Commonwealth;
- identify the most effective means of international co-operation and enforcement, taking into account, amongst others the Council of Europe Convention on Cybercrime, without duplicating the work of other international bodies; and
- collaborate with other international and regional bodies with a view to identifying best practice, educational material and training programmes for investigators, prosecutors and judicial officers".

At a subsequent meeting in Perth, Australia (October 2011), the Commonwealth Heads of Government reiterated their commitment to improve national security by improving legislation and capacity in tackling cybercrime and other cyberspace security threats. Following this an intersectoral, inter-governmental Commonwealth Working Group on Cybercrime was established. The Working Group has been meeting regularly to explore and outline strategies on the following core elements of the mandate:

- Explore the practical implications of addressing cybercrime in the Commonwealth;
- Identify the most effective means of international cooperation and enforcement to combat cybercrime taking into account the work of other international organisations; and
- Identify best practices and educational materials and training programmes for training of criminal justice officials;

Though this is work in progress, the Working Group is expected to produce a draft report including recommendations for the consideration of the Meeting of Senior Officials scheduled to be held in October 2013, with a view to submitting a final report to the Meeting of Commonwealth Law Ministers in 2014.

There have also been various initiatives on the African continent as well as in its different regions to improve cybersecurity and combat cybercrime:

A Draft Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa is currently receiving attention under the auspices of the African Union.

In September 2012 a draft convention on cybercrime was approved by the 4th African Union Conference of Ministers responsible for ICT. The objectives of the draft convention are to harmonise legislation relating to e-transactions development, personal data protection, cyber security promotion and the fight against cybercrime. The Convention is expected to be in force from 2014.

The AU Commission is further collaborating with regional economic communities for harmonization of legislation for the East, Southern and North Africa Unions.

In this regard we can mention that last year the Southern African Development Community (SADC) and the ITU ran a regional initiative aimed at harmonising legal frameworks for Southern Africa, in particular legal frameworks relating to Electronic Transactions, Protection of Personal Data and Cybercrime.

In April 2012, the Economic Community of West African States (ECOWAS) was urged to establish a convention on cybercrime for the Region. A resolution passed at the three-day regional workshop on cyber-crime organised by the Economic and Financial Commission, (EFCC) of Nigeria, and the Australian Federal Police, AFP. The conference also deliberated on the need for practical cooperation among West African countries in terms of policing and intelligence gathering on cybercrime-related issues and other organized crimes and called on law enforcement agencies in the region to come together and think up policies on how to tackle the issue of cybercrime.

The move towards international and regional conventions has at heart the objective to ensure that we harmonise our legal frameworks to ensure that we can act in concert against cyber threats perpetrated against any one of the member states. It also aims to provide member states with frameworks on the type of issues that need to be embraced by respective national cybersecurity laws.

In South Africa we have various domestic laws dealing with cyber issues whether in the enforcement of copyright law regarding the downloading of music, or the application of the general principles of contract law to online contracts, or the rules relating to e-filing, digital signatures. It is also highly significant in dealing with the combating of criminal aspects such as pornography, cyber-stalking etc.

We also have international agreements/treaties ranging from bi-lateral and multi-lateral mutual legal assistance treaties and instruments to specific international agreements on substantive law elements such as patent law.

I will attempt a brief overview of the relevant legislative provisions or laws we have in place to cover ICTs / internet related issues.

The Constitution of the RSA, 1996, informs all other legislation or law which has to conform to the entrenched constitutional values or norms. This is especially relevant to aspects such as the right to privacy, the right to freedom of expression and the right of access to information.

The Promotion of Access to Information Act, 2000 (Act 2 of 2000) also known as PAIA, allows in particular access to both written and electronic records of information that can include personal information. It also deals with unreasonable privacy infringements.

The Electronic Communications and Transactions Act, 2002 (Act 25 of 2002) (ECT Act) is the cornerstone of our ICTs or cyberlaw in South Africa and covers a wide variety of topics in one omnibus Act.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002) (RICA) deals with the interception and monitoring of information and the provision of communication-related information in SA.

The Electronic Communications Act, 2005 (Act 36 of 2005) and the Independent Communications Authority of South Africa Act, 2000 (Act 13 of 2000) deal with convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors and provide a legal framework for these sectors ensuring regulation of electronic communication services, network and broadcasting services and the provision of licenses etc.

The Protection of Personal Information Bill, 2009 (Bill B9 of 2009). This Bill aims amongst others to promote the protection of personal information processed by public and private bodies, codes of conduct, and to regulate the flow of personal information across the borders of the RSA.

Protection Against Harassment Bill â€“ Cyber-stalking

I want stress that the legislation I mentioned represents only the most significant enactments that in my view directly relate to the growing body of Law in this subject matter.

Many other enactments have been made to keep abreast of advances in technology or ICTs. Examples in this regard relate to electronic contracting, e-commerce, software patents, copyright, trade marks, domain names and dispute resolution, online consumer protection, etc.

In future many more legislative developments may follow especially regarding cybercrime and electronic evidence.

It is clear that not only domestic law but also international law and conventions will in future have increasing relevance regarding cyber-related aspects and your conference and the topics on the agenda is thus of great value.

From our Government's point of view, the ensuring of cybersecurity and the combating of cybercrime remains key priorities. Specific JCPS Cluster activities in this regard are therefore part and parcel of our commitments under Outcome 3: "All people in South Africa are and feel safe". Outcome 3 has very specific outputs dealing with cyber-security and cybercrime, namely -

- A safer cyber space; and
- Reduced cybercrime.

To help deal with these aspects a National Cybersecurity Policy Framework (NCPF) was developed to ensure a focussed and an all-embracing safety and security response in respect of the cyber security environment. This was approved by Cabinet on 7 March 2012. In summary, this framework outlines policy positions and activities that are intended to:

a) Address national security threats in cyberspace;
b) Combat cyber warfare, cybercrime and other 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 information and communication technologies.

In particular, the Policy Framework provides for the following:

- The development and implementation of a Government led, coherent and integrated cyber-security approach to address Cyber-security threats;
- Establishing a dedicated policy, strategy and decision making body known as the JCPS Cybersecurity Response Committee, to identify and prioritise areas of intervention and focussed attention regarding cyber security related threats. The Cybersecurity Response Committee is chaired by the State Security Agency (SSA).

- The capability to effectively coordinate departmental resources in the achievement of common cybersecurity safety and security objectives (including the planning, response coordination and monitoring and evaluation);
- Fighting cyber crime effectively through the promotion of coordinated approaches and planning and the creation of required staffing and infrastructure;
- Coordination of the promotion of cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) in relation to cybersecurity threats, through interaction with and in conjunction with the Cybersecurity Hub (led by the Department of Communications);
- Strengthening of intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;
- Ensuring of the protection of national critical information infrastructure;
- The promotion of a cybersecurity culture and compliance with minimum security standards;
- The establishment of public-private partnerships for national and action plans in line with the NCPF; and
- Ensuring a comprehensive legal framework governing cyberspace.

The State Security Agency is leading the the implementation of this Framework.

Unfortunately I cannot deal with all aspects of the Framework. However, good progress is being made in implementing its key aspects. For example:

The Cybersecurity Response Committee, chaired by the State Security Agency (SSA) is meeting regularly;

A draft cybercrime policy framework has been developed by the law enforcement agencies and is currently under consideration in the Cluster.

The Cybersecurity Hub is in the process of being implemented by the Department of Communication and should be in operation during 2013/14.

A review of legislation pertaining to cyberlaw aspects has been initiated in the Department of Justice and Constitutional Development with an inter-sectoral team currently doing desktop research, international comparative studies and engaging in consultations with academics and legal practitioners and other role players aimed for later in 2013.

A number of SAPS and DPCI staff members as well as more than 175 prosecutors have been trained regarding cybercrime issues; and

Various cybercrime cases have further been investigated and taken to court. For the current financial year till the end of February 2013, 123 such cases were prosecuted with a 97,6% conviction rate

Since 2008 there were a number of instances of 'cyber heists' where victims suffered losses of millions of Rand.

Experience has taught that the most effective response is pro-active intelligence driven criminal investigations.

Three examples illustrate this point:

Firstly, S v Morwesi Theledi: In this case R27 million was stolen in December 2009. As a result of pro-active investigations law enforcement alerted the relevant bank and its customer of this crime before they themselves were even aware of it. The stolen amount was transferred back into the account of the victim and only R18 000 was lost. The accused was arrested and after a long trial convicted and sentenced to 10 years imprisonment. She spent two years in jail awaiting trial. Bail was successfully opposed by the state.

Secondly, the Postbank Case: In this case R42 million was stolen during the period 1-3 January 2012. Four persons were arrested. Three of the accused were sentenced to various terms of imprisonment, each of which must serve at least 10 years. The fourth accused is awaiting trial.

Thirdly, during May 2009 a criminal syndicate hacked into the account of a state department (DOJ). Information was received about their activities and their unlawful electronic transfers were blocked with the assistance of the relevant bank. R16 million was illegally transferred but law enforcement managed to prevent this loss. The crime took place late on a Saturday evening but thanks to the effective communication and public-private partnership the crime was detected and disrupted in real time.

These examples illustrate that cyber threats are real but also that the seriousness with which our Justice, Crime Prevention and Security Cluster is taking these threats is not virtual, it is very real. Those serving sentences will attest to the fact that they are not playing a computer game in prison.

In conclusion, we wish to stress the point that applies to so many other crime and security threats: the need for co-operation, partnerships and public awareness.

In this regard we again wish to express our support for this initiatives and look forward to its outcomes as a contribution to ensure that All in South Africa are Safe and Feel Safe, also in cyberspace.

I thank you.

Back ◀

NEWSROOM
- Home
- Speeches & Statements
- Conferences/Workshops
- Events
- Call for Public Comment
- Videos