PARLIAMENT
OF THE REPUBLIC OF SOUTH AFRICA

RESEARCH UNIT
PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 8273 Fax: 27 (21) 403 8118
www.parliament.gov.za

21 August 2017

DEPARTMENT OF TELECOMMUNICATIONS AND POSTAL SERIVCES: CYBERSECURITY

1. INTRODUCTION

South Africa established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. The hub enhances interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society.

This paper will provides an overview of Cybersecurity in South Africa and what the Department of Telecommunications and Postal Services is doing to ensure that South Africa is cyber secure.

2. CYBERSECURITY IN SOUTH AFRICA

Cybersecurity involves protecting information and systems from major cyber threats, such as cyber terrorism, cyber warfare and cyber espionage. In their most disruptive form, cyber threats are aimed at secret, political, military, or infrastructural assets of a nation, or its people. Cybersecurity is therefore a critical part of any governments' security strategy.

Cybersecurity should be understood within the context of information warfare. The South African National Defence Force (SANDF) defines information warfare as actions executed to ensure the protection of the military's information based processes, information systems and communication networks, and to destroy or neutralise the adversary's similar capabilities within the physical, information and cognitive domains in order to gain an edge during war.

According to cyber security experts, cyber-attacks are a growing risk to business in South Africa. Although it is argued that neither the government nor business is doing enough to combat it, however, South Africa has made positive advances. Cyber-crime has a negative effect on South Africa's productivity, national security and its attractiveness as an investment destination. According to Basie Von Solms, Director of the University of Johannesburg's Centre for Cyber Security, the shortage of skills combined with a lack of urgency in implementing measures to tackle cybercrime have seen South Africa rank low on a number of cyber security assessments. In the 2013 the Norton Report found that South Africa has the third-highest number of cyber-crime victims, after Russia and China. Von Solms argues that cyber-crime is largely unregulated by government agencies. Although business should also play a part in tackling cyber-crime, government should take the lead.

2.1. The National Cyber Security Policy Framework

The Cabinet passed the National Cyber Security Policy Framework in March 2012. The aim of the framework is:

- Promoting a cyber-security culture and demanding compliance with minimum standards;
- Strengthening intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber warfare, cyber terrorism and other cyber ills;
- Establishing public-private-societal partnerships for national and international action plans;
- Ensuring the protection of National Critical Information Infrastructure (NCII);
- Promoting and ensure a comprehensive legal framework governing cyberspace; and
- Ensuring adequate national capacity to develop and protect cyberspace.

The framework implementation is supported by a number of institutional mechanisms, which include:

I. The Cyber Security Response Committee
II. Cyber Security Centre
III. Cyber Security Hub
IV. National Computer Security Incidence Response Team (NCSIRT) and sector CSIRTs
V. National Verification of Information Security Products and Systems
VI. Protection of the National Critical Information Infrastructure (NCII).

2.2. National Cyber Security Advisory Council

In terms of the National Cyber Security Policy Framework (NCPF), South Africa established the National Cyber Security Advisory Council (NCAC) on 15 October 2013. The roles of the NCAC are the following:

- Advising the Minister of Communications on policy issues and other matters pertinent to cybersecurity;
- Promoting intergovernmental cooperation on cybersecurity matters;
- Promoting and encourage coordinated private – public partnerships on issues regarding cyber security in the country;
- Assessing the state of national cybersecurity, determine needs and advise on appropriate responses and priorities; and
- Providing oversight regarding the implementation of national cybersecurity initiatives and structures.

Currently, the NCAC is headed by Dr. Barend Taute, and other members including Deputy Chairperson Ms Ritasha Jethva, Mr Sizwe Snail, Mr. Collen Weapond, Mr Mark Heyink, Prof Tana Pistorius and Dr. Khomotso Kganyago. Although NCAC has been established, South Africa's Computer Security Incident Response Teams (CSIRTs) are still being developed under the State Security Agency. In Africa, only Tunisia, Mauritius and Kenya have fully active CSIRTs. The establishment of the NCAC, however, indicates the country's seriousness in terms of cyber security.

2.3. Organisations dealing with Cyber Security

In terms of cyber security, there are several departments and concomitant organisations who are responsible. These include the Department of Telecommunications and Postal Services, the SANDF, the Centre for Scientific and Industrial Research (CSIR), the State Security Agency (Domestic and Foreign Branch), the South African Police Service (SAPS), the Special Investigative Unit (Hawks), and the State Information Technology Agency (SITA).

Although the Act governing cyber security mandates the Department of Telecommunications and Postal Services as the leading department, the SANDF is charged with protecting South Africa against any external threat. As such SANDF is responsible for the military aspects of cyber-defence and cyber warfare. The 2014 Defence Review states that for South Africa to protect itself in the cyberspace there is a need to adapt with the rapidly changing electronic environment. The National Cyber-Security Policy Framework sets out a number of tasks directly aligned to the Department of Defence, which include, inter alia, addressing national security threats in cyber-space, combating cyber-warfare, cyber-crime and other cyber ills; developing, review and update existing substantive and procedural laws to ensure alignment; and building confidence and trust in the secure use of information and communication technologies. The Cyber-Security Response Committee of the Justice Crime Prevention and Security Cluster (JCPS) coordinate all South African cyber-security activities. The Department of Defence (DOD) has overall responsibility for the coordination, accountability and implementation of cyber defence measures in South Africa as an integral part of its constitutional mandate.

A number of other organisations also have roles to play in cyber security. The CSIR conducts research into cyber-warfare for the government and the SANDF. The roles of the State Security Agency include providing intelligence and counter intelligence services to fight cyber-warfare; while those of the SAPS and the Hawks' role include cyber-crime and fraud. SITA provides the government with information technologies.

3. SOUTH AFRICA'S CYBERSECURITY READINESS

In order to ensure that South Africa is cyber secure, the Department of Telecommunications and Postal Services have undertaken certain initiatives to ensure South Africa is safeguarded from cyber-attacks. The following provides an overview of the presentation to be given to the Portfolio Committee by the Department on Cybersecurity.

The Minister of Telecommunications and Postal Services officially opened the Cybersecurity Hub on 30 October 2015. The responsibilities of the Cybersecurity Hub according to the NCPF is as follows:

- Consultation – the hub needs to ensure appropriate consultation between the JCPS cluster departments, the private sector and civil society regarding cybersecurity matters.

- Co-ordination – coordinate general cybersecurity activities; identifying stakeholders and developing public-private relationships and collaborating with any sector CSIRTs that may be established.
- Disseminate information – disseminate relevant information to sector CSIRTs, vendors, technology experts.
- Provide guidance – provide best practice guidance on ICT security for Government, business and civil society.
- Promote compliance – promote compliance with standards, procedures and policy and best practices
- Create awareness – initiate cybersecurity awareness campaign.

Computer Security Incident Response Teams (CSIRTs) are teams of dedicated information security specialists that prepares for and responds to Cybersecurity breaches or cybersecurity incidents. Over the years CSIRTs have extended their capacities and increased their service offerings, from being a reaction force to a complete security service provider. The cybersecurity hub coordinates with the sector CSIRTs, which includes telecoms, retail, finance, logistics, health, higher education and other sectors. Due to the various CSIRTs being established, the CSIRT Forum was formed in April 2017 with the intention to coordinate activities amongst the various CSIRTs.

Some of the other initiatives being undertaken to ensure South Africa is cyber secure include the following:

- Improved consultation and coordination – through the cybersecurity incident response 'war room'
- Investigate the development of 'home-grown' cybersecurity tools
- Piloting of a business intelligence solution
- Sector-specific Readiness Survey Current Initiative
- Development of National Standards and Guidelines
- Development of a national Cybersecurity Skills framework
- Development of a national Awareness Strategy
- Development of a national Awareness Portal
- Hosting of regional hackathons.

The above initiatives are being overseen by the Department of Telecommunications and Postal Services.

4. ISSUES FOR CONSIDERATION BY PARLIAMENT

- In the Cybersecurity Hub, how are cybersecurity incidents recorded and who alerts the hub to a cybersecurity threat? How is this threat responded too?

- The Committee should ask the Department to rate South Africa's readiness to deal a major cybersecurity threat.

- How far/to what extent have the initiatives listed above been implemented to strengthen cybersecurity in South Africa?

- The Department mentions two major global incidents in 2017, the ransomware WannaCry and Petya, on slide 22. How soon did South Africa become aware of these threats and how timeous was our response?

4. CONCLUSION

The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. South Africa established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The hub coordinates and consults with sector CSIRTs to ensure that South Africa is cyber secure. In addition to the Cybersecurity Hub, the Department is overseeing further initiatives to strengthen cybersecurity in South Africa.

5. REFERENCES

Cwele, SC. (2014) Minister of State Security, Republic of South Africa Cyber Security Meeting, Johannesburg 27 March 2014 [Internet], Available from: <http://www.ssa.gov.za/Portals/0/SSA%20docs/Speeches/2014/Minister%20Cwele%20Cyber%20Security%2027%20March%202014.pdf> (Accessed on 05 August 2014).

Department of Communications. (2009) Draft Cybersecurity Policy of South Africa: Pretoria: Department of Communications.

Department of Communications. (2013) Minister Inaugurates National Cyber Security Advisory Council [Internet], Available from: < http://www.doc.gov.za/mediaroom/media-statements/247-minister-inaugurates-national-cyber-security-advisory-council.html> (Accessed 12 August 2014).

Department of Defence. (2014) South African Defence Review 2014. Pretoria: Department of Defence.

Department of Telecommunications and Postal Services (2017) Cybersecurity, Briefing to the Portfolio Committee, 22 August 2017. Presentation to the Portfolio Committee on Telecommunications and Postal Services, Cape Town, Parliament of the Republic of South Africa.

Jones, G. (2014) South Africa neglects alarming effect of cybercrime [Internet], Available from: <http://www.bdlive.co.za/business/2014/01/14/south-africa-neglects-alarming-effect-of-cybercrime> (Accessed on 05 August 2014).

Palo Alto Networks (2016) What is cyber security? Available from: <https://www.paloaltonetworks.com/documentation/glossary/what-is-cyber-security> (Accessed on 17 November 2016)

State Security Agency. (2014) Computer Security Incident Response Team (CSIRT) [Internet], Available from: < http://www.ssa.gov.za/CSIRT.aspx> (Accessed on 15 August 2014).

Van Niekerk, B. and Maharaj, M. (2012) A South African Perspective on Cyber Warfare, in Cyber Conflict: Competing National Perspectives. Edited by Daniel Ventre London and New Jersey: ISTE Limited and John Willey and Sons.