PARLIAMENT
OF THE REPUBLIC OF SOUTH AFRICA

COMMITTEES
PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2597 Fax: 27 (21) 403 3205
www.parliament.gov.za

5 March 2020

CYBER SECURITY AND THE SOUTH AFRICAN NATIONAL DEFENCE FORCE

Author**|** Peter Daniels **Telephone|** 021 403 8450

1. INTRODUCTION

Cyber security is an issue that is being taken very seriously by both governmental and private sector agencies. In the last week of October 2019, the City of Johannesburg was subjected to a shut-down of its website after hackers exploited a hole in its information security protection. A demand was made of R450 000 worth of bitcoins. It was however not the first time that hackers have brought down a municipal site, as it happened in two other cases in the USA. On the other hand, Ukraine's power grid was taken down by hackers in 2016.[1] More alarming, is that more than a third of South African IT decision makers say they expect a cyberattack within at least two days, at any given time. Cyber-attacks are becoming the tactic of choice by those who like to strike from a distance and at a relatively low cost. Groups such as hostile foreign governments, activists, terrorists and criminals now use these tactics. "*Securing data should therefore be a priority for public and private institutions in the light of rapidly evolving threats*." If one considers that modern weapon systems are essentially embedded in software and information technology such as targeting systems, flight software and weapons-launching mechanisms, it is clear that this connectivity allows for advances in fighting wars, but also leaves these systems open to intrusion and disruption by adversaries.[2] As such, the "*Emergence and prevalence of Cyber Warfare threats*"[3] and especially its potential impact on defence infrastructure, facilities and information, is a matter that the Department of Defence should not only take seriously, but also have to take active steps against.

1.1 Definitions

There is not a general universal recognised definition of cybercrimes.[4] Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.

[1] Karen Allen, 2019. Cyber awareness must become part of every aspect of life from doing business to alleviating poverty and providing security. defenceWeb. https://www.dailymaverick.co.za/article/2019-06-26-is-africa-cyber-crime-savvy/?tl_inbound=1&tl_groups[0]=80895&tl_period_type=3&utm_medium=email&utm_campaign=Afternoon%20Thing%20Wednesday%2026%20June%202019%20Home%20Suite%20Hotels%20Bristol%20launch%20campaign&utm_content=Afternoon%20Thing%20Wednesday%2026%20June%202019%20Home%20Suite%20Hotels%20Bristol%20launch%20campaign+CID_10ecf81bbb6b6237f625a30d9dee4f64&utm_source=TouchBasePro&utm_term=ISS%20TODAY%20Is%20Africa%20cyber-crime-savvy. 26 June 2019

[2] Africa Defense Forum. 2020. A web of threats, a world of potential. 13 February. Accessed at https://www.defenceweb.co.za/cyber-defence/a-web-of-threats-a-world-of-potential/

[3] DOD, 2019. Annual Report of the Department of Defence FY 2018/19. P. 86

[4] Cybercrimes and Cybersecurity Bill [B6 – 2017] Memorandum. p. 63.

- **Operational security** includes the processes and decisions for handling and protecting data assets.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security
- practices.[5]

1.2 Cybersecurity

Cybersecurity can more readily be defined as technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or a computer systems against cybercrime, damage or interference.[6] Some are related to data, messages, computers, and networks. For example:

- hacking,
- unlawful interception of data,
- ransomware,
- cyber forgery and uttering, or
- cyber extortion.[7]

1.3 Prevalence of Cyber attacks

Cybersecurity concerns are present in all nations, but the exact nature of the threats differs depending on the country and/or region.[8] The U.S. government spends $19 billion per year [1] on cyber-security but warns that cyber-attacks continue to evolve at a rapid pace.[9] According to cyber analytics firm Kaspersky Lab, there are 13,842 cyber-attacks daily in South Africa. That equates to more than 570 attacks every hour. Bank fraud, particularly the use of malware on mobile phones, has also increased dramatically, says the South African Banking Risk Information Centre. Kenya is facing a similar problem. The Communications Authority has reported a dramatic rise with nine-million malware attacks in just three months from October to December 2018. Mobile phone subscriptions across sub-Saharan Africa are expected to reach 930 million by the end of 2019 and with the growth of e-commerce and e-banking continent-wide, the potential to inflict huge financial, reputational and political damage is clear. [10]

2. THE DEPARTMENT OF DEFENCE AND CYBER SECURITY

An effective mechanism against cyber-attacks, especially on defence facilities and infrastructure, appears to be taken seriously by the Department of Defence. In its MTSF 2015 – 2019 in Outcome 3: "*All people in South Africa are and feel safe*" in Sub-outcome 4, it refers to "*Secure Cyberspace*," and the establishment of a Cyber Command Centre Headquarters, scheduled

[5] Kaspersky, 2019. What is cyber security? Accessed at https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. On 12 November 2019

[6] Cybercrimes and Cybersecurity Bill [B6 – 2017] Memorandum. p. 63.

[7] https://www.michalsons.com/blog/cybercrimes-and-cybersecurity-bill-the-cac-bill/16344

[8] Brett van Niekerk, 2017. An Analysis of Cyber-Incidents in South Africa. An analysis of cyber-incidents in South Africa. The African Journal of Information and Communication (AJIC), 20, 113-132.

[9] Kaspersky, 2019

[10] Karen Allen, 2019.

for FY2018/19. As part of the Justice Crime Prevention and Security Cluster (JCPS) it contributes towards the development of National Cyber security.[11] This after the DOD 2017 Annual Performance Plan planned a Cyber Command headquarters that was to be set up in the 2018/19 financial year.[12]

The importance of having a working cyber defence strategy in place has been emphasised by defence analyst Helmoed Romer Heitman. "*The potential consequences of a major cyber-attack in terms of damage to the economy and to the ability of the country to function are such that this should be regarded as part of the defence domain. This is an intelligence-heavy area, so the requisite intelligence and protection/defence capabilities, and the development or pre-emptive and counter-strike capabilities, should for now lie with Defence Intelligence.*" he said. It is partly with this in mind that the DOD has set annual targets related to Cyber security in its annual performance plans.

2.1 Annual Target

The DOD 2017[13] had an annual target to the develop of a Cyber Warfare Strategy for approval by the JCPS Cluster namely "Cyber Warfare Strategy submitted for approval by the JCPS Cluster Ministers." The actual performance on this target is indicated as "*The Cyber Warfare Strategy is in the departmental approval process*" and the mitigating factor is given as *"Implementation of the Cyber Warfare Strategy will commence once it is approved*." [14] It would thus be important that the Portfolio Committee follows up how this target will be accommodated in the 2020 – 2025 MTSF.

Defence Intelligence Programme Performance Status for FY2018/19		
Link to Strategy Map	**Performance Indicator**	**Analysis**
	Level of Implementation of the Cyber Warfare Plan57	**Target** Phases 4 – 5 **Actual** The Cyber Defence Action Plan (previously referred to as the Cyber Implementation Plan) in the departmental approval process. Phase 4 (Obtain Budget) and Phase 5 (Establish Capabilities) is in process. The Cyber Defence Action Plan (previously referred to as the Cyber Implementation Plan) is in the departmental approval process. Phase 1 (Establish HQ) – planning was concluded, however, the full establishment of a Cyber Command Centre was not achieved due to financial constraints. • Phase 2 (Finalise Functions) – planning in this regard was concluded, however, the finalisation of functions is dependent on the approval of the Cyber Warfare Plan.

[11] DOD, 2019. Department of Defence Annual Report FY2018/19. p. 39.

[12] https://www.defenceweb.co.za/cyber-defence/south-africa-pushing-cyber-defence/ 6 October 2017.

[13] https://www.defenceweb.co.za/cyber-defence/south-africa-pushing-cyber-defence/ 6 October 2017.

[14] DOD, 2019. Annual Report of the Department of Defence FY 2018/19. P. 86

		• Phase 3 (Finalise Structures) – planning in this regard was concluded, however, the finalisation of structures is dependent on the approval of the Cyber Warfare Plan. **Deviation** The Cyber Warfare Plan is still in the departmental approval process (awaiting approval of the Cyber Strategy).

The Cyber Command Center has not been established although it was to be fully operational in FY2018/19, due to monetary constraints. This target was part of the annual targets that Programme 7: Defence Intelligence was supposed to meet. It shows clearly the knock-on effect regarding the failure of Programme 1: Administration to develop the strategies timeously. It states that the reason this annual target was not met, was because *"The Cyber Warfare Plan is still in the departmental approval process (awaiting approval of the Cyber Strategy)."* [15]

6.2 Cyber Warfare threats

The DOD has been identified Cyber Warfare threats as an Enterprise Risk and indicated that it could not effectively deal with this challenge given the lack of funding in this regard, as can be viewed below.

DOD Enterprise Risk Management and Mitigation[16]	
Risk Response	**Risk Response Progress and Intervention**
Enterprise Risk 5 : *Emergence and prevalence of Cyber Warfare threats*	
Establishment and Maintenance of a Cyber-capability in the DOD	The DOD Cyber Strategy has been approved, however, the Cyber Project inclusive of the structure, remains unfunded.
The interim Cyber doctrine for the DOD approved and implemented	The DOD Cyber Strategy has been approved by the DOD and currently been submitted for Cluster approval. The doctrine will be included as part of the Cyber Implementation Plan. Notwithstanding the funding challenges, business, data and network vulnerability to possible cyber-attacks to the DOD remains.
Develop the DOD Cyber Warfare Policy in line with the National Cyber Policy	The DOD Cyber Implementation Plan is currently being developed and costed since the DOD Cyber Strategy has been approved. The process will also ensure that the DOD Cyber Policy is developed.

defenceWeb 2019 has reported in January 2018 already that due to a lack of funds, Defence Intelligence (DI) was not able to complete "*a full cyber warfare strategy could not be developed during the previous financial year, but a draft was completed*." They added that the level of implementation of the SANDF's cyber warfare plan is "in process" at phases two and three. [17]

[15] DOD, 2019. Annual Report of the Department of Defence FY 2018/19. P. 86

[16] DOD, 2019. Annual Report of the Department of Defence FY 2018/19. P. 141

[17] http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=50367:lack-of-funds-prevents-defence-intelligence-from-completing-cyber-warfare-strategy&catid=111:SA%20Defence&Itemid=242. 12 February 2018.

7. ARMSCOR AND THE COUNCIL FOR SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)

3.1 Armscor

Armscor, the defence acquisition agency, has created an in-house cybersecurity unit which plans to develop a globally competitive cyber warfare capability that will be a strategic reserve for the SA National Defence Force (SANDF).[18] This comes in the wake of it having suffered a cyber-attack. It was reported that “*Hackers affiliated with #OpAfrica compromised the state-owned arms procurement agency Armscor’s invoicing portal, releasing a number of purchasing information records.”*[19] The hacktivists allegedly used a “simple SQL injection” to breach this data and leak 63MB in HTML files on the dark web - a part of the internet that is not made public. The files are said to include ordering and payment details for companies ranging from Airbus, Thales Group, Rolls Royce and Denel. The Anonymous hacker also told HackRead.com that the hacktivists have access to 19 938 supplier IDs, names and their passwords. These passwords allow anyone to log in to the Armscor system as supplier or manager.[20]

Armscor is collaborating with the CSIR and Denel and they are apparently progressing on various aspects of South Africa’s ability to defend itself from cyberattacks, an area the Department of Defence (DoD) has allocated R72 million to over the medium term.[21] Armscor plans to protect itself and all the intellectual property residing within the agency from cyber-attacks via an information security department.[22] Armscor has identified three immediate cyber threats “likely to affect the defence industry” namely data breaches, malware deployed as an advanced persistent threat and artificial intelligence used for hacking.[23]

3.2 Council for Scientific and Industrial Research (CSIR)

The Council for Scientific and Industrial Research (CSIR) is promoting its wide array of cyber defence and security offerings, including a cyber test range, network simulator and cyber vulnerability detector. The Council’s Cyber Range is a virtualised environment with sensors that collect network data, hardware and software behaviour and user interactions as a test bed for cyber experts – or as a training simulator for incoming cybersecurity engineers.[24] In its latest annual report, the CSIR states it has developed two home-grown cybersecurity technologies in response to local and global cybersecurity challenges.

4 THE CYBER-CRIMES AND CYBER-SECURITY BILL ([B6 – 2017]

South Africa, as a leading economy in Africa, is acquiring new tools in its armoury to fight the criminals. The Cyber-crimes and Cyber-security Bill (2018) broadens the scope of cyber

[18] https://www.defenceweb.co.za/cyber-defence/armscor-cybersecurity-unit-up-and-operational/ dated 31 May 2019

[19] Van Zyl in Brett van Niekerk, 2017. See https://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712

[20] Gareth van Zyl, 2017. Anonymous ‘hacks’ Armscor website. 12 July 2016. Accessed at https://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712

[21] https://www.defenceweb.co.za/cyber-defence/south-africa-pushing-cyber-defence/ 6 October 2017.

[22] http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=50045:armscor-planning-to-arm-itself-against-cyber-attacks&catid=7:Industry&Itemid=116

[23] https://www.defenceweb.co.za/cyber-defence/armscor-cybersecurity-unit-up-and-operational/ 31 May 2019.

[24] https://www.defenceweb.co.za/cyber-defence/csir-enhances-cyber-offerings/ 23 May 2019.

offences as set out in earlier legislation, permits extradition and offers tougher sentences.[25] The Cybercrime Bill also creates many new offences. The primary aim of the Bill is to deal with cybercrimes and cybersecurity. As indicated above, there is not a general universal recognised definition of cybercrimes.

4.1 Department of Defence's role in terms of the Cybercrimes and Cybersecurity Bill

The references to the Department of Defence and its role with the Cybercrimes and Cybersecurity Bill are listed below to give an indication of what is expected of the DOD and to provide for possible questions in this regard. The Bill refers to the DOD as one of the representative Departments in Clause 53. It further states in Clause 54 entitled "Government structures supporting cyber security" that:

"(3) (a) The Cabinet member responsible for ***defence*** *must—*

> *(i) establish and maintain a cyber offensive and defensive capacity as part of the defence mandate of the South African National Defence Force; and (ii) in cooperation with any institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programs for members of the South African National Defence Force in order to give effect to subparagraph (i).*
>
> *(b) The Cabinet member responsible for defence may make regulations to regulate any aspect which is necessary or expedient for the proper implementation of this subsection.*
>
> *(c) The Cabinet member responsible for defence must, at the end of each financial year, submit a report to the Chairperson of the* ***Joint Standing Committee on Defence*** *of Parliament on the progress made with the implementation of this subsection."*

The Memorandum to the Bill repeats that: "*the Cabinet member responsible for defence must establish and maintain a cyber offensive and defensive capacity as part of the defence mandate of the South African National Defence Force.*"[26]

4.2 JSCD on the Cybercrimes and Cybersecurity Bill 2017

The DOD briefed the JSCD on the Cybercrimes and Cybersecurity Bill 2017 on 9 March 2019. It explained the mandate of the SANDF in terms of the National Cybersecurity Policy framework, its roles and responsibilities regarding the Bill, and steps taken to give effect to the Bill as well as the existing and planned initiatives relating to cybersecurity. The DOD stated that its mandate finds expression in five distinctive domains, Land, Sea, Air, Outerspace and Cyberspace. The principles of international law regulating the use of force must find expression in all these dimensions. Currently there is no clarity on what constitutes force in the context of Cyberwarfare across the five domains. [27]

The Cybercrimes and Cybersecurity Bill [B6 – 2017] should be viewed against the background that the Department of Defence has been mandated to develop a Cyber Warfare Strategy, to establish a DOD Cyber Security Incident Response Team (CSIRT), and to establish a Cyber Command Centre as R340 million has been budgeted for this.

[25] Karen Allen, 2019.

[26] Bill [B6 – 2017] Memorandum. p. 78.

[27] https://www.michalsons.com/blog/cybercrimes-and-cybersecurity-bill-the-cac-bill/16344

5. THE THREE COLOURFUL HACKERS

One of the terms that often comes up when engaging a topic like cyber security, is that of a hacker. Not all hackers are bad, and it is important to distinguish between the kinds of hackers. There are two main factors that determine the type of hacker you're dealing with: their motivations, and whether or not they are breaking the law. Three colours are used to distinguish between hackers, along the Western movies, namely a white (typically the hero), grey (uncertain till he makes his move) and the black hat (the villain).[28]

5.1 The black hat hackers

Like all hackers, black hat hackers usually have extensive knowledge about breaking into computer networks and bypassing security protocols. They are also responsible for writing malware, which is a method used to gain access to these systems. Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime. Black hat hackers can range from amateurs getting their feet wet by spreading malware, to experienced hackers that aim to steal data, specifically financial information, personal information and login credentials. Not only do black hat hackers seek to steal data, they also seek to modify or destroy data as well.

5.2 White Hat Hackers

White hat hackers choose to use their powers for good rather than evil. Also known as "ethical hackers," white hat hackers can sometimes be paid employees or contractors working for companies as security specialists that attempt to find security holes via hacking. White hat hackers employ the same methods of hacking as black hats, with one exception - they do it with permission from the owner of the system first, which makes the process completely legal. White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies. There are even courses, training, conferences and certifications for ethical hacking.

5.3 Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat activities. Often, grey hat hackers will look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the issue. If the owner does not respond or comply, then sometimes the hackers will post the newly found exploit online for the world to see. These types of hackers are not inherently malicious with their intentions; they're just looking to get something out of their discoveries for themselves. Usually, grey hat hackers will not exploit the found vulnerabilities. However, this type of hacking is still considered illegal because the hacker did not receive permission from the owner prior to attempting to attack the system.[29]

[28] https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html. Accessed 5 November 2019.

[29] https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html. Accessed 5 November 2019.

6. POSSIBLE QUESTIONS

- What is the latest regarding the establishment of the Cyber Warfare Plan?
- What kind of support does Department receive from both the CSIR and Denel to strengthen its Cyber security?
- Have any cyber security breaches taken place in the Department? If yes, was it contained and have measures been put in place to prevent a re-occurrence?
- Has Armscor sufficiently addressed the security weakness that allowed hackers to compromise its system?
- Did the breach at Armscor have any impact on the delivery of services and goods to the DOD?
- The Portfolio Committee should follow up on the target "*Implementation of the Cyber Warfare Strategy*" in the 2020 – 2025 MTSF.
- If the Cybercrimes and Cybersecurity Bill is passed, the JSCD should ensure that the Minister submits an annual report on the Department's cyber offensive and defensive capacity.

7. CONCLUSION

Cyber security is an issue that all countries are grappling with to secure their facilities and infrastructure, given the damage that cyber-attacks can cause. If one has regard for the essentiality of the defence force and the need to keep some of its facilities and especially plans secure, it is evident that our military needs to operate in a secure cyber space. While the DOD has been tasked to build a cyber offensive and defensive capacity and to develop a Cyber Command as part of the Intelligence Division, this has not materialised primarily due to a lack of funding. The Cybercrimes and Cybersecurity Bill however reinforces the role of the DOD in this domain and it is therefore incumbent that the necessary attention and urgency should be paid to address the lack of progress in developing mechanisms to protect especially the DOD against cyberattacks.