Stiftung Neue Verantwortung

Exercise Background Material

South Africa

Country Profile

Points of Contact: Rebecca Beigel, Julia Schuetze | Stiftung Neue Verantwortung e. V.
Beisheim Center | Berliner Freiheit 2 | 10785 Berlin

Disclaimer:

The research only represents a country's cybersecurity policy to a limited extent and is not an in-depth or complete analysis or assessment of current policy. In order to adapt the exercises to specific countries, it is important to understand the broader strokes of cybersecurity policies of other countries. Our team, therefore, researches publicly available information on cybersecurity policies of countries to adapt the exercises to country-specific needs. The research is shared with participants as background material in preparation for the exercise. Therefore, the documents have a timestamp and consider policy up until the date of publication. In the interests of non-profitability, we decided to make the background research publicly available. If you are using these materials, please include the disclaimer. Please also do not hesitate to contact us.

Points of Contact:

Rebecca Beigel

Project Manager for International Cybersecurity Policy

rbeigel@stiftung-nv.de

+49 (0)30 40 36 76 98 3

Julia Schuetze

Junior Project Director for International Cybersecurity Policy

jschuetze@stiftung-nv.de

+49 (0)30 81 45 03 78 82

Table of Contents

1. South Africa – Political System and Socio-Political Background

Key Facts

- Official Country Name: The Republic of South Africa (RSA), Pretoria is the capital.[1]
- Population: population of about 58,56 million people (2019).[2]
- 11 official languages, among others, isiZulu, isiXhosa, Afrikaans, Sepedi, English.[3]
- Currency: South African Rand.[4]

Political System

- Form of Government: Parliamentary democracy with a strong presidency and federal elements.[5]
  - Head of State and Government: Cyril Ramaphosa, President of the Republic of South Africa, part of the African National Congress (ANC) party.[6]
    - Commander-in-Chief of the South African National Defence Force.[7]
    - Appoints deputy president to be the leader of government business in the National Assembly and appoints members of the cabinet.[8]
    - Government departments are organized in seven clusters to foster holistic and integrative governance.[9]
    - Elected by National Assembly from among its members.[10]
- Bicameral Legislature consisting of the National Assembly and the National Council of Provinces (NCOP).[11]

Socio-Political Context

- After the end of the apartheid regime in 1994, the African National Congress (ANC) party was elected with Nelson Mandela as South Africa's president.[12]
  - The ANC has controlled the government ever since the end of apartheid. Although it has held a majority in parliament, the ANC continues to lose support in municipal elections, especially in key urban areas.
  - The government faced the challenge of integrating the previously oppressed majority into the economy.[13]
  - From 2009 onwards, Jacob Zuma filed for the position of South African president. Zuma resigned in 2018 after being involved in several corruption scandals.[14]
- South Africa has the highest level of inequality worldwide.[15]
  - RSAs unemployment is significantly higher than the average for emerging markets, especially youth unemployment.[16]
  - Economic inequality inherited by the apartheid regime further expanded during the early 2000s. [17]
  - This inequality also contains a digital divide. Internet users are primarily urban and affluent citizens. While Internet access is available primarily in rural areas since the early 2000s, people can often not afford computers or do not have the skills to work with them.[18]
- In the World Economic Forum's Global Competitiveness Report 2019, RSA's Adoption of Internet Communication Technologies (ICTs) ranks 89th out of 141 countries.
  - Around 56.2% of adults use the internet (89.7% in Germany).
  - Digital skills among its active population rank especially low on place 126 out of 141, indicating the width of South Africa's digital divide.[19]

Vulnerability and Threat Landscape

South Africa has in the past been an outstandingly high victim of various cyber-attacks. According to a report by Accenture, South Africa has the third-highest number of cyber-crime victims worldwide. Cybercrime amounts to an economic loss of $147 Million US-Dollars a year.[20] The report analyses that threat actors rarely mentioned South Africa in the dark web until 2014. Only in 2016, threat actors increasingly started to focus on the RSA. In general, cyberattacks of all kinds are now consistent with other world economies.[21] However, the rapid increase in mobile banking apps has made financial service apps prone to attacks[22] with South Africa being the second-most targeted country for Android banking malware in 2019.[23]

The following exemplary cases of cyber-attacks gained national and international media attention:

- In July 2019, a ransomware attack hit a large **electricity supplier in Johannesburg.** The company‘s IT systems were shut down. Databases and networks were encrypted.[24] While the website went offline, several citizens reported power outages and could not buy pre-paid electricity. A city spokesperson said that approximately more than a quarter of a million people were affected.[25]

- In September 2019, several **internet service providers (ISP) were hit four times by several significant carpet bomb attacks.** Carpet bombing is a special kind of DDoS technique by which traffic is sent to random IP addresses in an ISP‘s network. Contrarily, to a direct DDoS attack on the ISP‘s servers, the systems could not detect the traffic until the company‘s plans crashed.[26] The attacks occurred over several days and did target other ISPs as well.[27]

- In October 2019, Johannesburg‘s computer network of the **city government was attacked by a perceived ransom attack.** The criminals named „Shadow Kill Hackers“ hacked into the government network and demanded four bitcoins (nearly $32,000 US-Dollars at the time) not to publish compromised data.[28] Authorities immediately shut down IT infrastructure, including all e-services, and confirmed that the network was breached. According to a city spokesperson, no critical data was affected because the network was breached at the user level.[29] The city did not pay a ransom and decided to restore its computer network. A city council member announced: „[T]he City will not concede to their demands, and we are confident that we will be able to restore systems to full functionality.“[30]

2. Overview: South Africa‘s Cybersecurity Policy

Cybersecurity Policy

According to the Global Cybersecurity Index (GCI) 2020, the RSA ranks eighth in the African region regarding its commitment to cybersecurity policy.[31] The GCI is calculated by the International Telecommunications Union (ITU) based on five pillars containing, for instance, legal measures or international cooperation.[32]

South Africa‘s interest in cyberspace is primarily defined by the **National Cybersecurity Policy Framework (NCPF)** across various sectors – the most crucial being security, defense, and telecommunications.[33] The **NCPF** was adopted by the South African Government in 2012. It sets out to coordinate a coherent cybersecurity approach across ministries and government agencies.[34] The State Security Agency (SSA), an agency that provides intelligence on foreign and domestic threats, is responsible for implementing the NCPF.[35]

The primary concern is to ensure confidentiality, integrity, and availability of computer data and systems. Consequently, the NCPF sets out to prevent and address cybercrime, strengthen intelligence collection, and protecting national critical information infrastructure.[36]

The NCPF aims to enhance coordination between government institutions. To increase the efficiency of coordinating departmental resources, the NCPF envisions various new institutions to strengthen cybersecurity:

- A **JCPS Cybersecurity Response Committee** that acts as a dedicated policy-, strategy-, and decision-making body. This committee will be chaired by the SSA and supported operationally by a Cybersecurity Centre within the SSA.
- A National **Cybersecurity Hub** that should be established within the DTPS to promote cybersecurity coordination with all stakeholders (public sector, private sector, and civil society).
- A **National Cybersecurity Advisory Council (NCAC)** advising that the Minister of Telecommunications and Postal Services on policy issues and technical issues of cybersecurity.
- A **Cyberwarfare Command Centre HQ** that will be established by the DoD.[37]

The framework states that a wide range of activities at different levels is needed to ensure the security of a country's cyberspace. Among others, the NCPF envisions the following policies:

1. To establish a national information security verification framework and develop **regulations to verify ICT products** and systems.
2. To promote a national critical information infrastructure **(NCII) strategy** to develop regulation and protection for critical infrastructure.
3. To develop **cyber capacity-building strategies** and thus promote R&D.
4. To promote a cyber defense strategy by mandating the Department of Defence (DoD) to draft a **Cyber Warfare Strategy**.[38] However, according to the DoD 2019/2020 Annual Report, the Cyber Warfare Strategy has not yet been submitted to the Justice, Crime Prevention and Security Cluster (JCPS).[39]

Legal Framework

Legally cybersecurity and the prosecution of cybercrime are regulated through the **Electronic Communications and Transactions Act (ECTA)**. Cybercrime regulation will be additionally regulated by the **Cybercrimes Bill** that was signed into law in June 2021 and is currently awaiting its commencement date.[40]

The **ECTA (No. 25 of 2002)** is currently the primary legislation governing cybersecurity policy in South Africa.[41] Among others, the ECT Act regulates electronic communication, and thereinafter aims to prevent the abuse of information systems. Specifically, Chapter XIII defines the issue of cybercrime and penalizes it. Section 86, article 2 states: „A person who intentionally [...] interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offense.“[42]

The **Cybercrimes Bill (No. B6D-2017)** defines in detail cybercrime matters and proposes regulations to coordinate the investigation of cybercrimes, impose obligations on reporting cybercrime, and provide capacity-building measures. The bill also allows the executive branch to enter into any cybersecurity agreements with foreign states[43]

The bill was previously introduced as **Cybercrimes and Cybersecurity Bill (No. B6 2017)** in 2017 but was met with considerable public criticism.[44] While it was criticized that the cybersecurity section of the bill would provide for extensive powers of the South African government and was unconstitutional, the chapter on cybercrime was reintroduced as Cybercrimes Bill.[45]

Cybersecurity Architecture - Selected Institutions

The NCPF mandates existing institutions with tasks and establishes the objective to create new institutions and mandate existing institutions with new tasks. Existing institutions with a mandate in cyberspace are the **Department of Communications and Digital Technologies (DCDT), the State Security Agency (SSA)**, the **Department of Defence (DoD)**, and t**he South African Police Service (SAPS)**. The **Electronic Communications Security – Computer Security Incident Response Team (ESC-CSIRT)**, which works with various government institutions, is hosted within the SSA. Additionally, the NCPF mandates the creation of multiple institutions, including the **National Cybersecurity Advisory Council (NCAC)**, the **National Cybersecurity Hub**, and the **Cyberwarfare Command Centre HQ**. Functions of all institutions are discussed below:

The **DTPS** was remodeled into the **Department of Communications and Digital Technologies (DCDT)** in June 2019.[46] The DCDTs mission is to create an ICT environment that promotes socio-economic development and investment. Regarding cybersecurity, the department aims to provide a „robust, reliable, secure and affordable ICT infrastructure.“[47] Internally, the DTPS has a Chief Director for Cybersecurity Operations[48] responsible for the national cybersecurity mandate and the national CSIRT.[49]

The **State Security Agency (SSA)** is the government‘s department supervising all civilian intelligence operations. Its mandate includes intelligence on foreign and domestic threats that pose a danger to „national stability, the constitutional order, and the safety and well-being of [South Africans].“[50] The SSA was responsible for drafting the NCPF in 2012. As envisioned in the NCPF, a **Cybersecurity Response Committee** chaired by the SSA and a supporting **Cybersecurity Centre** hosted by the SSA were proposed to facilitate government structures against cybercrimes[51]. These institutions were initially written into law by the Cybersecurity and Cybercrimes Bill (B6-2017)[52] but were not reiterated in the Cybercrimes Bill (B6D-2017)[53]. Future implementation is unclear.

Additionally, the SSA hosts the **Electronic Communications Security – Computer Security Incident Response Team (ESC-CSIRT)**, established in 2003.[54] While the National Cybersecurity Hub serves as a CSIRT for all South African stakeholders, the ECS-CSIRT serves as the CSIRT of the South African Government and offers its services as a single point of contact to entities of the RSA‘s state.[55]

The NCPF mandated the **DoD** to draft a Cyber Warfare Strategy. The DoD also planned to establish a **Cyberwarfare Command Centre HQ**[56]. However, there is no publicly available information on its establishment. The Annual Report for the DoD‘s financial year 2019/2020 shows that a Strategy is being drafted but has not yet been finalized since 2016. A Command Centre is not mentioned.[57]

The **South African Police Service (SAPS)** is mandated by the NCPF with preventing, investigating, and combating cybercrime as well as with the development of cybercrime policies and strategies.[58] In the context of cybercrimes committed inside or outside South Africa, the SAPS established a 24/7 Point of Contact for “requests from, or to, foreign countries/entities”.[59]

As mandated by the NCPF, the **National Cybersecurity Advisory Council (NCAC)** is a body of seven members from all stakeholder groups who advise the Minister of the DTPS (now the DCDT) on all cybersecurity matters.[60] These include advice on policy, legal and technical issues (i.e., adopting standards in the RSA, developing an annual report, establishing a Cybersecurity Hub, and matters referred to by all ministers).[61]

As mandated by the NCPF, the **National Cybersecurity Hub** was established in 2015 by the DTPS.[62] The Hub is the countries' Computer Security Incidence Response Team (CSIRT) and acts as a central point of contact to (a) prevent IT security incidents and (b) respond to them. The Cybersecurity Hub serves as a platform for all stakeholders to collaborate on IT issues. By responding to the incident, the Hub aims at building confidence in South Africa's ICT environment.[63]

Bilateral and Multilateral Cooperation

South Africa is a member of the African Union (AU), the Commonwealth, the International Telecommunications Union, and the United Nations (UN).[64] All these international organizations deal with and discuss cybersecurity-related topics. The AU, for example, adopted the **Convention on Cyber Security and Personal Data Protection (Malabo Convention)** in 2014 to address cybersecurity and cybercrime.[65] However, South Africa has not yet signed the Malabo Convention.[66]

South Africa signed the Budapest Convention on Cybercrime (Treaty No. 185) with its inception in 2001 but has not ratified it yet.[67] The Budapest Convention is the first international treaty to pursue a standard criminal policy through cooperation and legislation against cybercrime.[68]

- The convention mandates signing entities to adopt legislation that penalizes various cybercrimes (Art. 2 – Art. 10), for instance, illegal access of computer systems, computer-related fraud, and copyright infringements.[69]
- States are mandated to adopt legislation that makes investigations into cyber-related crimes possible. States are, for instance, required to adopt legislation that allows competent authorities to collect and record traffic and content data in real-time (Art. 20 & Art. 21).[70]
- According to chapter III of the convention signing, states are subject to cooperate in fighting cybercrime. States are asked to afford other parties the most comprehensive mutual assistance possible in investigating cybercrimes. Under the convention, the extradition of individuals that have committed cybercrimes between states is possible. Additionally, states are asked to share information and evidence and stored computer data and traffic data to investigate cybercrimes.[71]
- To facilitate cooperation and mutual assistance, states are asked to provide a 24/7 hour-point of contact that can provide technical advice and has the authority to share information and evidence on behalf of the party (Art. 35).[72]

Within the UN, South Africa is also part of the 2019-2021 **Group of Governmental Experts (GGE)** on advancing responsible state behavior in cyberspace in the context of international security. The GGE debates behind closed doors on how international law and norms should be applied in cyberspace and how capacity and confidence can be built. Countries are asked to appoint representative experts to the group meetings held behind closed doors. Representatives are, in most cases, government officials with either technical or diplomatic backgrounds. The GGE will present its final report in September 2021.[73]

Additionally, South Africa is part of the **Open-Ended Working Group (OEWG) on Developments in the Field of ICTs in the Context of International Security**, established in 2018. The OEWG is (as opposed to the GGE) open to all UN members and establishes a continuing dialogue on cybersecurity issues within the UN.[74] In its final report in March 2021, the OEWG supported the notion that international law and the UN Charter should be applica-

ble in cyberspace and that states should voluntarily identify and cooperate on confidence-building measures in their local contexts. South Africa's input and comments on the draft of the final report are available online. It highlights its approval of the report and remarks that it remains open to establishing institutions that facilitate dialogue on cybersecurity.[75]

Regarding bilateral cooperation, South Africa maintains several agreements with third states.

- The South African telecommunications minister concluded a **cooperation agreement with Iran** in 2017. The agreement aims to increase joint investments and R&D, among others in cybersecurity.[76]
- A **cooperation agreement with Russia** was signed by the foreign minister in 2017. Both states aim to maintain international information security and commit to working jointly on responding to and investigating threats in cyberspace. The agreement also allows both states to coordinate approaches within international organizations like the UN.[77]
- An **MoU with the French Embassy** was signed by the South African Special Investigation Unit (SIU) in 2017, a state agency to fight corruption. The MoU commits to training 350 forensic investigators on the expertise of cybercrime.

Sources

1 Auswärtiges Amt: Überblick. Südafrika. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/suedafrika-node/suedafrika/208382

2 World Bank: Population, South Africa. https://data.worldbank.org/indicator/SP.POP.TOTL?locations=ZA

3 Auswärtiges Amt: Überblick. Südafrika. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/suedafrika-node/suedafrika/208382

4 Global Exchange: South African Rand. https://www.globalexchange.es/en/currencies-of-the-world/south-african-rand

5 Auswärtiges Amt: Überblick. Südafrika. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/suedafrika-node/suedafrika/208382

6 Ibid.

7 Presidency of South Africa: Address by Commander-In-Chief, President Cyril Ramaphosa, on the occasion of Armed Forces Day 2020, Polokwane, Limpopo: http://www.thepresidency.gov.za/speeches/address-commander-chief%2C-president-cyril-ramaphosa%2C-occasion-armed-forces-day-2020%2C

8 South African Government: Executive Authority. https://www.gov.za/about-government/government-system/executive-authority-president-cabinet-and-deputy-ministers

9 South African Government: Government clusters. https://www.gov.za/government-clusters.

10 South African Government: Government clusters. https://www.gov.za/government-clusters.

11 South African Government: National legislature (Parliament). https://www.gov.za/about-government/government-system/national-legislature-parliament

12 Britannica: African National Congress. https://www.britannica.com/topic/African-National-Congress/Internal-dissent

13 Britannica: Economy of South Africa. https://www.britannica.com/place/South-Africa/Economy

14 Ibid.

15 International Monetary Fund (2020): IMF Country Focus. https://www.imf.org/en/News/Articles/2020/01/29/na012820six-charts-on-south-africas-persistent-and-multi-faceted-inequality

16 Ibid.

17 Britannica: Economy of South Africa.
https://www.britannica.com/place/South-Africa/Economy

18 Enrico Calandro (2020): Observing global cyber norms nationally -the case of critical infrastructure protection in South Africa.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895156
SANGONeT (2020): Levels of Digital Divide in South Africa.
http://www.ngopulse.org/article/2020/08/28/levels-digital-divide-south-africa

19 Schwab (2019): The Global Competitiveness Report 2019.
http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

20 Accenture (2020): Insight into the cyberthreat landscape in South Africa
https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa

21 Ibid.

22 Ibid.

23 Shapshak (2019): South Africa Has Second Most Android Banking Malware Attacks As Cyber Crime Increases. https://www.forbes.com/sites/tobyshapshak/2019/05/09south-africa-has-second-most-android-banking-malware-attacks-as-cyber-crime-increases/?sh=15acdaba5d77

24 Janjevic (2019): Johannesburg power company hit by ransomware attack.
https://www.dw.com/en/johannesburg-power-company-hit-by-ransomware-attack/a-49741227

25 BBC (2019): Ransomware hits Johannesburg electricity supply.
https://www.bbc.com/news/technology-49125853

26 Cimpanu (2019): 'Carpet-bombing' DDoS attack takes down South African ISP for an entire day. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

27 Vermeulen (2019): Massive DDoS attacks – South African Internet providers crippled.
https://mybroadband.co.za/news/internet/329539-massive-ddos-attacks-south-african-internet-providers-crippled.html

28 Cimpanu (2019): City of Johannesburg held for ransom by hacker gang.
https://www.zdnet.com/article/city-of-johannesburg-held-for-ransom-by-hacker-gang/

29 MIT Technology Review (2019) Hackers shut down Johannesburg's networks once again.
https://www.technologyreview.com/2019/10/25/132179/hackers-shut-down-johannesburgs-networks-once-again/

30 Montalbano (2019): City of Johannesburg, on Second Hit, Refuses to Pay Ransom.
https://threatpost.com/johannesburg-refuses-ransom-pay/149676/

31 ITU (2020): Global Cybersecurity Index 2020.

32 ITU (2020): Global Cybersecurity Index.
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

33 Sutherland (2017): Governance of Cybersecurity – The Case of South Africa. http://www.scielo.org.za/pdf/ajic/v20/05.pdf

34 SSA (2015): The National Cybersecurity Policy Framework (NCPF). https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

35 Government of South Africa: State Security Agency (SSA). https://nationalgovernment.co.za/units/view/42/state-security-agency-ssa

36 SSA (2015): The National Cybersecurity Policy Framework (NCPF). https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

37 SSA (2015): The National Cybersecurity Policy Framework (NCPF). https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

38 SSA (2015): The National Cybersecurity Policy Framework (NCPF). https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

39 DoD (2019): Annual Report FY 2019/2020. https://static.pmg.org.za/DOD_AR_2019-20_Web_20Nov20.pdf

40 ENSafrica (2021): The Cybercrimes Act Signed Into Law and Awaiting Commencement Date | South Africa. https://iclg.com/briefing/16439-the-cybercrimes-act-signed-into-law-and-awaiting-commencement-date-south-africa

41 UNIDIR: South Africa. https://unidir.org/cpp/en/states/southafrica

42 Government of South Africa (2002): Electronic Communications and Transactions Act. https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

43 Republic of South Africa: Cybercrimes Bill (B6D-2017). https://static.pmg.org.za/parl-bills-B6D-2017-GJ_B6D-2017-GJ.PDF

44 Parliament of the Republic of South Africa (2020): NCOP passed the Cybercrimes Bill, Civil Union and the Science and Technology Laws Amendment Bills. https://www.parliament.gov.za/press-releases/ncop-passed-cybercrimes-bill-civil-union-and-science-and-technology-laws-amendment-bills

45 Bhagattjee, Preeta / Govuza, Aphindile (2020): The Cybercrimes Bill is one step away from becoming law (Cliffe Dekker Hofmeyr). https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html.

46 National Government of South Africa: Department of Communications and Digital Technologies (DCDT). https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

47 DTPS: Mandates. https://www.dtps.gov.za/index.php?option=com_content&view=article&id=12&Itemid=165

48 DTPS (2017) Invitation to nominate members of the national Cybersecurity Advisory Council https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National-Cyber-Security-Advisory-Council.pdf

49 CSSA2019: Keynote Speakers. https://cssa.ac.za/cssa2019/

50 Government of South Africa: State Security Agency (SSA). https://nationalgovernment.co.za/units/view/42/state-security-agency-ssa

51 SSA (2015): The National Cybersecurity Policy Framework (NCPF). https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

52 Republic of South Africa: Cybersecurity and Cybercrimes Bill (B6D-2017). https://static.pmg.org.za/170221b_6_-_2017_cybercrimes.pdf

53 Republic of South Africa: Cybercrimes Bill (B6D-2017). https://static.pmg.org.za/parl-bills-B6D-2017-GJ_B6D-2017-GJ.PDF

54 FIRST: ECS-CSIRT. https://www.first.org/members/teams/ecs-csirt

55 UNIDIR: South Africa. https://unidir.org/cpp/en/states/southafrica

56 Martin, Guy (2017): https://www.defenceweb.co.za/cyber-defence/department-of-defence-aims-to-beef-up-cyber-security/

57 DoD (2019/2020): Annual Report. https://static.pmg.org.za/DOD_AR_2019-20_Web_20Nov20.pdf

58 South African Police Service (2018): PRESENTATION TO THE PORTFOLIO COMMITTEE ON JUSTICE AND CORRECTIONAL SERVICES CYBERCRIMES AND CYBER SECURITY BILL [B6-2017]. https://pmg.org.za/files/180213SAPS.pptx

59 Ibid.

60 South African Government (2013): Minister inaugurates National Cyber Security Advisory Council. https://www.gov.za/minister-inaugurates-national-cyber-security-advisory-council

61 DTPS: Terms of Reference for the National Cybersecurity Advisory Council. https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/NCAC-ToR-2017-Reappointment_V1.pdf

62 Prio (2021): Inside South Africa's Cybersecurity Hub. https://mybroadband.co.za/news/security/379370-inside-south-africas-cybersecurity-hub.html

63 Cybersecurity Hub (n.d.): The Cybersecurity Hub. https://www.cybersecurityhub.gov.za/ UNIDIR: South Africa. https://unidir.org/cpp/en/states/southafrica

64 UNIDIR: South Africa. https://unidir.org/cpp/en/states/southafrica

65 CCDCOE: African Union. https://ccdcoe.org/organisations/au/

66 African Union (2020): Ratifying countries. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

67 Council of Europe (2020): [South Africa] Cybercrime legislation. https://rm.coe.int/octocom-legal-profile-south-africa/16809e952d

68 Council of Europe (2004): Details of Treaty No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

69 Council of Europe (2001): Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

70 Ibid.

71 Ibid.

72 Ibid.

73 Digwatch: UN GGE and OEWG. https://dig.watch/processes/un-gge

74 Ibid.

75 South Africa: South Africa's inputs and comments on the "Pre-draft" of the report of the OEWG on development in the Field of Information and Telecommunications in the context of International Security. https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/South+Africa%E2%80%99s+Inputs+and+Comments+on+the+%E2%80%9CPre-Draft%E2%80%9D+of+the+Report+of+the+OEWG+on+Development+in+the+-Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security.pdf

76 Tasnim News Agency (2017): Iran, South Africa Agree to Boost ICT Cooperation. https://www.tasnimnews.com/en/news/2017/09/27/1531891/iran-south-africa-agree-to-boost-ict-cooperation

77 Ministry of Foreign Affairs of the Russian Federation (2017): Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security. https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2854430