THREAT LANDSCAPE:

Republic of South Africa (RSA)

Government:	Parliamentary Republic
Capital:	Pretoria
Chief of State:	President Cyril Ramaphosa
Natural Resources:	Gold, coal, chrome, antimonium, iron ore, manganese, nickel, phosphates, tin, uranium, diamonds, platinum, copper, vanadium, salt, natural gas
Societal Grievances:	Inequality[1], racial tension, xenophobia, violence against women, HIV/AIDs
APT Groups:	APT10, Operation Socialist (NSA and GCHQ), Equation Group[2], Careto APT[3]
Hacktivist Groups:	Anonymous South Africa, Anonymous Africa
Extremist Groups:	Right Wing Militia groups, Islamic extremist groups[4]
Criminal Groups:	Americans gang, Hard Livings gang, Bad Boys gang, Terrible Josters, Sexy Boys gang, Numbers Gang [5] [6]
Malware Families:	RoughTed, Fireball, Globeimposter, Cerber, Hummingbird, Hiddad, Triada, Dyre, Citidel, Trickbot, Kins

International Threat Landscape

Post-apartheid, South Africa sought to become a leading actor in the global economy. Today South Africa is the second largest economy in the African region and is a member of the BRICs bloc of countries (Brazil, Russia, India, China, and South Africa)[7]. Its biggest trading partners are Zambia, Japan and China[8]. South Africa and Nigeria are regional rivals for hegemony and the role of leadership on the continent[9]. Since Jacob Zuma assumed the presidency, South Africa has provided support in three conflicts; the Battle of Bangui in the Central African Republic, the M23 Rebellion in the Democratic Republic of Congo (DRC), and the ongoing Allied Democratic Forces (ADF) Insurgency in Uganda and the DRC[10]. However, South Africa is not involved in any direct military conflicts. South Africa was a member of the non-aligned movement during the cold war which sought to counter the competing power blocs of the USSR and the USA. Before the fall of the Berlin Wall and the ending of the Cold War, the primary national and international security threats were nuclear and revolutionary war. International organized crime has taken an interest in areas such as Kruger National Park, which is home to rhinoceros. The poaching and smuggling of wildlife can be linked to a number of international criminal groups including nation states such as North Korea. This is because of the lucrative value of animal parts such as the

[1] https://www.theguardian.com/inequality/datablog/2017/apr/26/inequality-index-where-are-the-worlds-most-unequal-countries

[2] http://it-online.co.za/2016/06/08/targeted-attacks-hit-sa-organisations/

[3] https://securelist.com/the-caretomask-apt-frequently-asked-questions/58254/

[4] https://issafrica.s3.amazonaws.com/site/uploads/sareport7.pdf

[5] https://www.vice.com/en_uk/article/4wbyqg/stars-stripes-and-blood-south-africas-most-notorious-gang-is-called-the-americans

[6] http://www.nigeriatoday.ng/2017/07/heres-how-the-gang-violence-in-cape-town-is-interconnected-infographic/

[7] http://www.academicjournals.org/journal/AJPSIR/article-full-text-pdf/00990B962911

[8] https://www.globalsecurity.org/military/world/rsa/forrel.htm

[9] http://cco.ndu.edu/Portals/96/Documents/prism/prism_5-2/PRISM5-2_Security_Threats.pdf

[10] https://www.globalsecurity.org/military/world/para/adf.htm

rhinoceros horn and abalone on the black market. Much of the poached abalone is destined for Hong Kong[11].

Domestic Threat landscape

South Africa has been called the “protest capital of the world”. According to statistics from the South African Police Service Data, on average 900 community protests a year occurred between 1997 and 2013. This climbed to 2000 annually in recent years[12]. Many of them have been violent. This trend reflects increasing domestic grievances and societal tension in marginalized communities who feel that economic hardship stems from racial inequality[13]. During 2016 there were widespread, violent protests following a government announcement relating to university fee increases[14]. Under the hashtag #feesmustfall, many of those protesting felt that the increase was discriminatory because it would take away opportunities for further education from black families with a lower average income than white families[15]. Hacktivist groups such as Anonymous South Africa have acted in alignment with these issues, conducting online and physical protests against President Jacob Zuma in #OpFreeSA and #SaveSA in 2016 and April 2017. Social issues and hacktivism have been intrinsically linked for some time[16].

South Africa has a “complex history of far-right extremism”. This was traditionally based on Afrikaner nationalism. Groups such as Afrikaner Weerstandsbeweging (AWB), Boere Aanvalstroepe and People Against Gangsterism and Drugs (PAGAD) have conducted attacks including shootings and bombings. There have also been links to international extremist organizations from individuals hiding in or travelling from South Africa. An estimated 60 – 100 South Africans went to join ISIS in Iraq and Syria. Current far-right groups such as Kommandokorps are still supportive of racial segregation[17].Right-wing militia groups such as Boeremag are enabled by technologies to conduct and coordinate activities. Online forums such as StormFront have South African members and help to bring these like-minded people together[18].

Crime rates in South Africa are particularly high and have increased in recent years. Between 2016 and 2017 on an average day: 2.1 people were murdered, 109.1 rapes were recorded, 428.6 people were victims of common assault, 61.2 households were robbed, and 386.2 robberies occurred with some kind of gun or weapon[19].

Cyber Threat Landscape Overview

South Africa was elevated to number 21 in a list of countries worldwide on the Threat Impact index in May 2017 by Check Point. Whilst Zambia, Nigeria, Uganda and Malawi were ranked worse, South Africa was placed 9th overall in Africa[20]. Sophos reports that across Africa Cerber accounts for 80% of all ransomware followed by Wannacry, Jaff, Locky and Petya. According to the Threat Impact index, South Africa is most concerned about the following malware families: RoughTed, Fireball and Globeimposter[21]. RoughTed is a large-scale malvertising campaign, whilst Fireball takes over browsers.
Mobile malware was dominated by Android malware; Hummingbird, Hiddad, and Triada are reported to be amongst the “most wanted” list[22].

Critical National Infrastructure

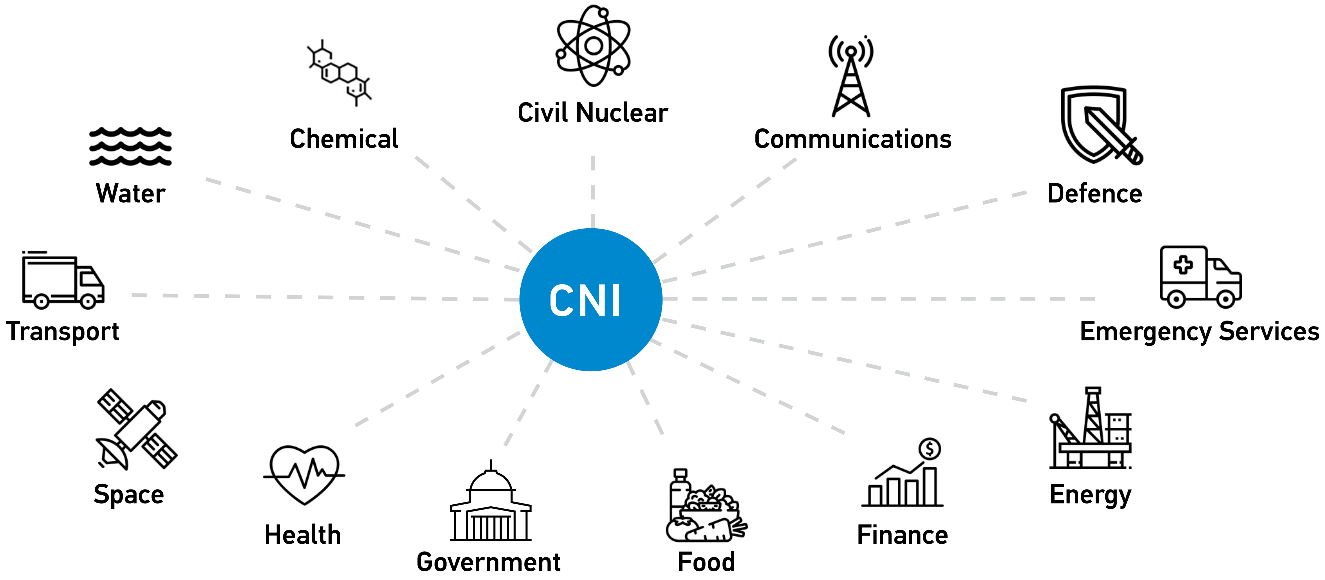
The following sections take a glance at the sectors deemed to be critical national infrastructure (CNI)[23]. CNI “are those facilities, systems, sites, information, people, networks, processes necessary for a country to function and upon which daily life depends”[24]. They can include the following areas: Chemicals, Civil Nuclear,

[11] http://www.traffic.org/home/2014/10/8/organized-crime-drugs-and-poverty-are-behind-south-africas-a.html
[12] https://www.iol.co.za/pretoria-news/sa-is-protest-capital-of-the-world-9279206
[13] http://www.worldbank.org/en/country/southafrica/overview
[14] https://www.amnesty.org/en/countries/africa/south-africa/report-south-africa/
[15] http://www.bbc.com/news/world-africa-34615004
[16] https://www.jbaynews.com/sa-police-website-hacked-by-anonymous/
[17] https://issafrica.s3.amazonaws.com/site/uploads/sareport7.pdf
[18] http://icsa.cs.up.ac.za/issa/2010/Proceedings/Research/02_paper.pdf
[19] https://africacheck.org/factsheets/south-africas-crime-statistics-201617/
[20] https://www.africa.com/five-worlds-highest-risk-countries-africa-according-check-points-latest-threat-index/
[21] http://www.itnewsafrica.com/2017/09/roughted-remains-the-top-malware-in-africa-to-watch-out-for/
[22] https://www.africa.com/five-worlds-highest-risk-countries-africa-according-check-points-latest-threat-index/
[23] The CNI sectors have been taken from the UK CPNI as a template.
[24] https://www.cpni.gov.uk/critical-national-infrastructure-0

Communications, Defense, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Because the functional well-being of the state is dependent on the services in these areas, an attack on any of the sectors will have a particularly high impact.

Summary of Findings

There are a few sectors that appear to be dominated by only one or two companies. Some of these companies overlap into other sectors of the CNI, which could indicate that to significantly disrupt South Africa, attackers only need to compromise a few targets on their list. The chemicals industry (alongside many other industries) is heavily reliant on water, which South Africa is experiencing an increasing shortage of after successive years of drought. Furthermore, the chemicals industry seems to be largely focused on the gasification of natural coal reserves, which then helps to generate 95% of South Africa's electricity. Eskom is the dominant supplier of electricity. Eskom operates a number of power stations and the only nuclear power plant. Armscor, who had taken part in the facilitation and production of nuclear weapons for South Africa during the cold war, is now the acquisition organization for Defense. Because of Armscor's history in successfully developing nuclear weapons (before dismantling them) and because of the country's reservoir of highly enriched uranium, this may be an area of targeting for physical attack, cyber espionage, or theft. Telkom is the only provider of fixed line communications and there are only three major cellular providers. Denel is the largest manufacturer for defense and a key supplier to the South African National Defense Force (SANDF). Any one of these organizations is an attractive target in order to undermine South Africa's critical infrastructure.



Chemical

Represented by:	Chemical and Allied Industries Association (CAIA) 135 members
Locations of Industry:	Gauteng (47%), KwaZulu-Natal (18%), Western Cape (16%)
Subsectors:	Liquid Fuels (31%), Plastic Products (20%), Inorganic Chemicals (8%), Pharmaceuticals (8%), Primary Polymers and Rubbers (7%), Organic Chemicals (6%), Consumer Chemicals (5%), Rubber Products (5%), Bulk Formulated (5%), Specialty Chemicals (5%), Fine Chemicals (1%)
Primary Focus:	Gasification of national coal reserves
Companies:	SASOL, Foskor, PetroSA
GDP Sector:	Comes under "Manufacturing" (13.4% of total GDP)

Summary of Industry

The Chemical Industry in South Africa is of noteworthy importance to the South African economy. It contributes heavily to the manufacturing sector and impacts the development of other industrial sectors such as agriculture, healthcare, clothing, and textile. "The chemicals sector in South Africa is the largest of its kind in Africa."[25] Petrochemicals make up 55% of the chemical industry. 92% of the coal consumed on the African content is produced in South Africa. 95% of South Africa's electricity is generated by burning coal. Shale gas, if proven to be commercially viable, will attract investment. Urea is not manufactured in South Africa presently.

Threats to Industry

The South African chemical industry relies heavily on water yet South Africa is one of the 30 driest countries in the world. Sasol scored a 4 (5 being the worst) in a 2017 Cyber Exposure Index (CEI) study, which indicated they had high amounts of leaked credentials and sensitive information (among other issues). [26] [27]

Notable Cyber Attacks

- In 2014, state-owned electricity provider Eskom's payroll system was hacked by employees, but the employees were prevented from making transfers by Eskom's anti-corruption units.[28]
- Approximately 20 websites, including Sasol, were defaced by a Moroccan hacktivist in 2014 who was protesting the South African position on the Western Sahara.[29]

[25] https://www.aiche.org/sites/default/files/cep/20150746.pdf

[26] http://www.pressreader.com/south-africa/the-citizen-kzn/20171017/281960312982956

[27] https://www.peta.ai/report/sasol

[28] http://www.cyberseo.co.za/latest-cyber-news/eskom-payroll-hack.html

[29] http://www.pressreader.com/south-africa/the-citizen-kzn/20171017/281960312982956

Civil Nuclear

Represented by:	Nuclear Energy Corporation of South Africa (Necsa)
Locations of Industry:	Koeberg near Cape Town & Durban, Thyspunt
Regulated by:	National Nuclear Regulator (NNR)
Companies:	UraMin (Uranium), Eskom (electricity)

Summary of Industry

South Africa's nuclear industry is heavily dependent on coal. Due to this dependency, power plants are built near the mines. South Africa gets 40% of its oil/gasoline needs from coal-to-liquids plants. South Africa's coal reserves are concentrated in Mpumalanga, whilst much of the need is near Cape Town and Durban. The Koeberg plant was built by Framatime (now Areva). The government plans to extend Koebergs operating life from 30 – 40 years. Eskom awarded the contract to install six new steam generators to Areva for 2017-18. In November 2013, Necsa signed a broad agreement with Russia's NIAEP-Atomstroyexport and its subsidiary Nukem Technologies to develop a strategic partnership. This included nuclear power plants and waste management, with financial assistance from Russia. In October 2014, a nuclear cooperation agreement with France was signed. In November 2014, a similar intergovernmental cooperation agreement was signed with China.

South Africa developed and built six nuclear weapons from 1982 – 1989. However, under the de Klerk government, the nuclear materials in Armscor's possession were returned to the Atomic Energy Corporation, where they were stored according to internationally accepted procedures. Armscor's facilities were decontaminated and dedicated to non-nuclear commercial purposes. The nuclear weapons program was dismantled by 1991. However, South Africa is a producer, possessor, and exporter of nuclear materials and technologies. The country still possesses a large quantity of highly enriched uranium (HEU) but has recently made progress in HEU minimization. The nuclear industry is lobbying to restart the countries enrichment program[30].

Threats to Industry

South Africa has a history with nuclear weapons, and the technology and knowledge has somewhat remained after denuclearization. This may make industry a target of aspiring groups and countries that could benefit from such information and resources.

Notable Cyber Attacks

In 2014, state-owned electricity provider Eskom's payroll system was hacked by employees but the employees were prevented from making transfers by Eskom's anti-corruption units[31].

[30] http://www.nti.org/learn/countries/south-africa/nuclear/

[31] http://wiredspace.wits.ac.za/bitstream/handle/10539/23573/AJIC-Issue-20-2017-Van%20Niekerk.pdf?sequence=3

Communications

Locations of Industry:	Undersea cables (WACS, SAT3, MainOne, EASSy and Seacom) appear to be located in Yzerfontein, Melkbosstrand and Mtunzini
Subsectors:	Mobile communications, internet, fixed-line communications
Companies:	Telkom (fixed-line communications), Neotel, Vodacom, MTN and Cell C (cellular services), Sentech (Broadcasting)
GDP Contribution:	Contributes approximately 10% of GDP

Summary of Industry

South Africa has had one of the fastest growing communications industries. This sector has seen accelerated growth compared to other national industries. Telkom has monopolized the supply of fixed-line communications, and its largest shareholder is the government. There are currently three major cellular service providers: Vodacom, MTN and Cell C.[32] [33]

Threats to Industry

The telecommunications industry could be negatively impacted by plans put forward in a Information and Communications Technology (ICT) policy white paper. The plans include the creation of an open-access national network with unallocated mobile spectrum. It includes proposals to request the acquisition of existing spectrum allocations thereby nationalising the network. This has created uncertainty for investors in cellular network providers active in South Africa[34].

Notable Cyber Attacks

- Telkom was hit by WannaCry ransomware in 2016[35].
- APT10 (China) has targeted Managed Service Provider (MSP) infrastructure allowing the group to move laterally onto MSP customer networks. South Africa was one of the regions impacted[36] [37].
- Operation Socialist (NSA and GCHQ) targeted Belgacom subsidiary BICS — a joint venture between SA MTN and Swisscom. Motives suggested that infecting the carrier service, which covers hotspots like Syria, could allow the agencies to track phone users (2014)[38].
- A flaw in mobile operator Vodacom's portal allowed any subscriber to access high level account summary information linked to any phone number[39].
- Customer records were accessible when a flaw was discovered in mobile operator Cell C's portal[40].
- Sensitive information was found accessible in the e-billing portal of mobile operator MTN.[41]
- In 2013, mobile operator MTN and affiliated service providers suffered a service outage due to a DDoS attack[42].
- In 2016, Anonymous Africa targeted the South African Broadcasting Corporation (SABC) with a DDoS attack making their website unavailable. The hackers stated that the attack was in protest against corruption and their belief that the network was censoring protests[43].

[32] https://www.ptycompanyregistration.co.za/communications-industry-south-africa/
[33] https://manypossibilities.net/african-undersea-cables/
[34] https://techcentral.co.za/sas-mobile-industry-is-under-threat/71296/
[35] https://businesstech.co.za/news/telecommunications/176067/telkom-hit-in-global-cyber-attack/
[36] https://media.scmagazine.com/documents/292/cloud-hopper-report-final-upda_72977.pdf
[37] https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
[38] https://www.scmagazineuk.com/belgacom-says-alleged-gchq-apt-attack-cost-firm-12-million/article/541153/
[39] https://mybroadband.co.za/news/security/94234-my-vodacom-security-flaw-exposes-subscriber-details.html
[40] https://mybroadband.co.za/news/security/94332-big-cell-c-security-flaw-uncovered.html
[41] https://mybroadband.co.za/news/security/94554-e-toll-website-flaw-a-cyber-attack-sanral.html
[42] http://www.telecomspeak.com/2015/05/18/cyber-attack-targets-mtn-data-centre
[43] https://mybroadband.co.za/news/security/168303-this-is-how-i-took-down-the-sabc-anonymous-hacker.html

Defense

Represented by:	Department of Defense, SANDF
Websites:	dod.mil.za, army.mil.za, navy.mil.za, af.mil.za, rfdiv.mil.za, mhs.mil.za, sf.mil.za
Subsectors:	SA Airforce, SAArmy, SANavy, Defense Intelligence, Joint Operations, SA Military Health Service, SA Special Forces
Primary Focus:	Oversees the military departments responsible for the defense of South Africa
Acquisition Organisation:	Armscor
Defense Suppliers:	Denel, Paramount Group, Reutech Radar Systems

Summary of Industry

The South African National Defense Force (SANDF) comprises the medical service, army, navy and airforce. Its domestic acquisition company is Armscor and it has a number of domestic and foreign suppliers. Denel is the largest South African Defense manufacturer. The Military strength of South Africa is currently ranked at 46 out of 133 countries in the Global Firepower Review[44].

Threats to Industry

The South African Department of Defense (DoD) has been hit with continuing budget cuts. Defense force capabilities are in decline[45], and budget cuts means that SANDF is picking up responsibilities that were once outsourced[46]. Evolving threats that SANDF and the DoD have to contend with include: cooperation with South African Police forces to help deal with protests in the run up to the 2019 election, naval operations on the West coast of Africa to counter piracy, and further cooperation with Namibia and Angola[47].

Notable Cyber Attacks

- Defacements on military websites occurred in 2001 and 2006 by "PoizonB0x", and Iranian hacker "old.zone".
- In July 2016, Anonymous breached the website of the South African government-owned arms supplier Armscor exposing information about defense manufacturers such as Denel, Thales Group, and Airbus. Armscor has claimed that after conducting an examination of the unauthorized access "no classified information was accessed"[48].

[44] https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=south-africa

[45] http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=48693&catid=74&Itemid=30

[46] https://www.businesslive.co.za/bd/national/2017-07-25-sandf-warns-budget-cuts-a-threat-to-sas-safety/

[47] http://www.janes.com/article/74823/south-african-military-looking-at-evolving-threats

[48] https://www.itweb.co.za/content/KwbrpOqgL4BvDLZn

Emergency Services

Represented by:	Department of Health
Websites:	ams.org.za, saesi.com, ndmc.gov.za, kishugu.com, saps.gov.za
Locations of Industry:	Local services
Areas of Concern:	Medical services, Fire service, Police, HAWKs
Technology:	Namola App
Companies:	Netcare 911, ER24, South African Ambulance and Emergency Services Association
Trade Union:	Health and Other Services Personnel Trade Union of South Africa

Summary of Industry

Netcare 911 and ER24 are privately-run emergency services which include ambulance services and a network of national hospitals. Netcare 911 includes road assistance and helicopter services. There is a government service called Emergency Management Service (EMS) which handles fire and ambulance services. Cities also have their own dedicated fire departments[49]. The South African Police Service was established over 100 years ago.

Threats to Industry

Emergency services have come under threat of robbery and physical attacks. Civilians in need of hospital admission have died as a result of these attacks and some areas have proposed the withdrawal of emergency services as a result[50].

Notable Cyber Attacks

- In 2013, the South African Police Services website was targeted, and information was stolen from the mail server. The information (which contained the details of victims and whistle-blowers) was uploaded and dumped onto another site. The site was vulnerable to an SQL injection attack[51].
- In 2010, a state hospital in the Western Cape was found to have an insecure site and thousands of patient records could have been accessed[52].

[49] http://country.southafrica.net/country/us/en/travel_tips/entry/emergency-services-enus

[50] https://www.news24.com/SouthAfrica/News/threat-to-withdraw-emergency-services-over-attacks-in-western-cape-20171109

[51] https://www.itweb.co.za/content/nG98YdqL2yx7X2PD

[52] http://wiredspace.wits.ac.za/bitstream/handle/10539/23573/AJIC-Issue-20-2017-Van%20Niekerk.pdf?sequence=3

Energy

Represented by:	Department of Energy (DoE)
Regulated by:	National Energy Regulator of South Africa (NERSA)
Subsectors:	Electricity, Coal, Nuclear, Wind, Solar, Hydro
Projects and Initiatives:	South African Smart Grid Initiative (SASGI), Integrated National Electrification Programme (INEP)
Companies:	Eskom
Suppliers:	137 Municipalities are distributing Eskom electricity to end-users

Summary of Industry

South Africa is part of SAPP (Southern Africa Power Pool). Eskom supplies about 95% of South Africa's electricity. Eskom also supplies about 45% of Africa's electricity. South Africa is contributing to the implementation of the Mozambique-Zimbabwe-South Africa (MOZISA) transmission project. Generation is currently dominated by coal power; however, this dominance is expected to decline in anticipation of increased investments in gas, renewables, and nuclear power[53].

Threats to Industry

The ongoing drought is likely to cause operational disruption. Hydropower accounts for around 20% of South African Power Pool (SAPP) common electricity market. In turn there is a greater risk of social unrest[54].

Notable Cyber Attacks

- Eskom's central electricity distribution network was declared "stupidly easy" to penetrate by Jacques van Heerden, owner of Global Technology Security Provider (GTSP)[55].
- In June 2017, Maersk Southern Africa was infected with Petya ransomware. The infection closed down "container shipping, port and tugboat operations, oil and gas production, drilling services and oil tankers.[56]"
- In 2013, the Department of Minerals and Energy lost over R 15 million after login credentials were stolen by criminals using a keystroke logging device[57].
- A South African petrochemical company's supervisory, control, and data acquisition system were infected by the PE Sality virus in 2009, denying the operator's visibility of operations for eight hours until the infected servers were recovered[58].

[53] https://www.africa-eu-renewables.org/market-information/south-africa/energy-sector/

[54] https://www.forbes.com/sites/riskmap/2016/02/04/drought-in-southern-africa-threatens-social-unrest-power-supply-challenges/#77e4e85e1ae6

[55] http://nationalcybersecuritynews.com/stupidly-easy-hackers-attack-eskom/

[56] http://www.ftwonline.co.za/article/123348/BREAKING-NEWS-Maersk-SA-hit-by-global-cyber-attack

[57] http://wiredspace.wits.ac.za/bitstream/handle/10539/23573/AJIC-Issue-20-2017-Van%20Niekerk.pdf?sequence=3

[58] http://wiredspace.wits.ac.za/bitstream/handle/10539/23573/AJIC-Issue-20-2017-Van%20Niekerk.pdf?sequence=3

Finance

Represented by:	Banking Association of South Africa
Central Bank:	South African Reserve Bank
Trading Market:	Johannesburg Stock Exchange (JSE)
“Big Five” Banks:	Absa, FNB, Standard Bank, Nedbank and Capitec
Legislation:	Banks Act 1990, Mutual Banks Act 1993
Regulatory Bodies:	Registrar of Banks (part of the reserve bank) , National Credit Regulator
Non-Banking Sectors:	Overseen by the Financial Services Board (FSB)

Summary of Industry

The financial sector is well regulated and competitive, attracting foreign banks and investment organizations. South Africa’s banking sector is comprised of 17 registered banks, 2 mutual banks, 2 cooperative banks, 43 foreign banks, and 14 local branches of foreign banks.

Threats to Industry

Macroeconomic uncertainty, technological risk, regulation and criminality (cyber-crime) are of concern to executives in this sector[59].

Notable Cyber Attacks

- In 2013, South Africa was been hit by Dexter malware, which led to one of the biggest cyber-fraud attacks in its history 2013[60].
- Hackers targeted three South African banks in 2006, managing to transfer cash from bank accounts into prepaid accounts held with mobile operators. It appeared that information was gained from keyloggers[61].
- In July 2009, a criminal group acquired, via threats to an engineer at Vodacom, duplicate SIM cards that allowed for interception of online banking one-time PIN codes (OTPs) for bank accounts they had compromised via phishing. They ended up stealing R 7 million from the compromised accounts[62].
- The Land Bank initially lost R 8 million stolen through fraudulent transfers in December 2010 after hackers compromised the bank’s IT security[63].
- A credit card payment provider, PayGate, was compromised in August 2012, affecting four of the major banks and compromising “hundreds of thousands” of credit card details[64].
- Postbank, the South African Post Office’s financial institution, had R 42 million stolen in January 2012 after hackers accessed servers via an employee’s workstation[65].
- In 2016, Standard Bank was targeted by hackers, who managed to steal approximately R 300,000,000 via ATMs in Japan[66]. Hackers are suspected to have broken into the banks system and taken approximately 3,000 sets of personal data. Forged cards were then prepared using the stolen data. Police in Japan later linked this attack with the Yakuza gang.

[59] https://www.pwc.co.za/en/press-room/banking-banana-skins.html

[60] http://www.bbc.co.uk/news/technology-24550505

[61] http://news.softpedia.com/news/Three-South-African-Banks-Hit-by-Hackers-28590.shtml

[62] http://www.thetimes.co.za/News/Article.aspx?id=1036132

[63] https://www.iol.co.za/business-report/companies/absa-intercepts-land-bank-swindle-1009423

[64] https://www.iol.co.za/personal-finance/my-money/banking/hack-attack-a-costly-lesson-for-banks-1425325

[65] https://www.itweb.co.za/content/kLgB1Me34VWv59N4

[66] https://www.reuters.com/article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB

Food

Represented by:	National Department of Agriculture, Forestry and Fisheries (DAFF)
Locations of Industry:	Food processing is located in urban areas
Subsectors:	Food processing, food and beverage manufacturing
International Companies:	Nestle, Unilever, Dole, Parmalat and McCain
National Companies:	Pioneer Foods, Tiger Foods, Distell, Capespan, Clover, Ceres Fruit Juices and SAB Miller (South African)
Union:	National African Farmers Union (NAFU)

Summary of Industry

South Africa has a very strong agricultural sector and is largely self-sufficient in fresh fruits and vegetables.

Threats to Industry

There is a dependence on other critical industries. For example, "an aseptic process plant cannot operate without a reliable electricity supply, complex machinery requires a source of skilled maintenance staff and processes depend on the consistent supply of ingredients of the correct specification." Arable land is also connected to historic discriminatory ownership from Apartheid. Land redistribution programs exist but the government has to balance maintaining public confidence in the land market whilst redistributing to the poor. The food industry is also precariously impacted by environmental issues such as drought. A report in 2015 outlined the future impact of many of these issues, pointing out that "South Africa is set to harvest its smallest maize crop in eight years owing to severe drought conditions in large productions areas."[67]

Notable Cyber Attacks

- A physical robbery at the Johannesburg offices for Nielson South Africa resulted in the theft of laptops, computers, and hard drives. Sensitive client information from the following companies was compromised: Unilever, SAB, Colgate, Distell, and British American Tobacco[68].

[67] http://www.wwf.org.za/?13521/Experts-caution-cause-for-alarm-in-future-of-SA-food-industry

[68] https://www.supermarket.co.za/news-article.asp?ID=7272&CatTags=17-Crime%20and%20security

Government

Composition:	Three branches of government (Legislative, Executive and Judicial)
Legislative:	Parliament, National Assembly and the National Council of Provinces
Executive:	Cabinet, President, Deputy President, Ministers, Provincial executive councils
Judicial:	Constitutional Court, Supreme Court of Appeal, High Courts, Magistrates courts, Judicial Service Commission
President:	Zuma, Jacob Gedleyihlekisa, Mr
Deputy President:	Ramaphosa, Matamela Cyril, Mr
Provinces:	Eastern Cape, Free State, Gauteng, KwaZulu-Natal, Limpopo, Mpumalanga, Northern Cape, North West, Western Cape

Summary of Industry

"South Africa is a constitutional democracy with a three-tier system of government and an independent judiciary."[69]

Threats to Industry

Corruption is a widely reported threat to the validity of South Africa's government. "Personal interests, greed and avarice continue to undermine the government's capacity to allocate resources effectively and to deliver services."[70]

Notable Cyber Attacks

- The Red October campaign was found to have mildly targeted South Africa[71], infecting a diplomatic organization[72].
- Zone-h.org shows 684 defacements for sites ending in ".gov.za" of which it considers 371 to be part of "mass defacements". Of those that have occurred in 2018, all have been submitted by an actor called "MuhmadEmad" who appears to be a Kurdish hacker conducting opportunistic defacements in support of the Kurds.
- The state's Government Communication and Information System (GCIS) was compromised shortly after V-Report, exposing the data of 1,500 government employees in #OpAfrica[73].
- In 2013, the website of the national ruling party, the African National Congress (ANC), was made inaccessible due to a distributed denial of service (DDoS) attack by Anonymous Africa[74].
- The Sednit/APT28 cyberespionage campaign, attributed to Russian hackers, targeted South African embassies via an infected document sent to the embassies purporting to be from the Department of International Relations and Cooperation[75].
- Three government websites were defaced by Moroccan hackers in 2012, protesting the official South Africa position on Western Sahara[76].

[69] https://www.gov.za/about-government/government-system/structure-and-functions-south-african-government

[70] http://www.wwf.org.za/?13521/Experts-caution-cause-for-alarm-in-future-of-SA-food-industry

[71] https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/

[72] https://securelist.com/the-red-october-campaign/57647/

[73] https://www.htxt.co.za/2016/02/12/anonymous-makes-good-on-promise-goes-after-sa-government-websites/

[74] http://www.securityweek.com/african-national-congress-website-hit-ddos-attack

[75] https://www2.fireeye.com/apt28.html

[76] https://mg.co.za/article/2012-12-09-three-government-websites-hacked

Health

Represented by:	Department of Health
Trust:	Health Systems Trust
Council:	Health Provisions Council of South Africa (HPCSA)
Health Issues:	HIV/AIDs
Initiatives:	National Insurance Scheme, roll-out of a standardised Electronic Patient Filing System, electronic stock management system
Distribution of Medicine:	Centralised Chronic Medicines Dispensing and Distribution programme
"Big 3" Hospital Groups:	Netcare Limited, Life Healthcare Group Limited, Mediclinic Southern Africa
Technology:	Namola App

Summary of Industry

South Africa's health system consists of a large public sector and a smaller but fast growing private sector. The private healthcare sector serves about 17% of the population[77]. The industry has reportedly shown growth as the government has promised more money for research and innovation[78]. The South African Health Review states that during its reporting history "HIV has been the highest priority preoccupation of service delivery."[79]

Threats to Industry

Corruption has been a problem in South Africa's health sector, based on a report that interviewed health sector informants. Evidence of corruption includes irregular expenditure.[80] [81] There are still challenges with overall maldistribution of financing between the private and public sectors.

Notable Cyber Attacks

- In 2010, a state hospital in the Western Cape was found to have an insecure site. Thousands of patient records could be accessed. [82]

[77] http://www.sharebox.co.za/a/4245

[78] https://www.marketopportunities.fi/innovative-solutions-for-the-south-african-health-care-sector

[79] www.hst.org.za/publications/.../HST%20SAHR%202017%20Web%20Version.pdf

[80] https://theconversation.com/south-africas-health-sector-is-leaking-money-what-can-be-done-about-it-45390

[81] https://www.wits.ac.za/media/news-migration/files/Presentation%20Dr%20Pieter%20de%20Jager%20SPH%20Symposium%20presentation.pdf

[82] http://wiredspace.wits.ac.za/bitstream/handle/10539/23573/AJIC-Issue-20-2017-Van%20Niekerk.pdf?sequence=3

Space

Represented by:	Department of Trade and Industry (DTI)
Regulation and Advisory:	South African Council for Space Affairs (SACSA)
Locations of Industry:	Pretoria, Gauteng
Space Agency:	South African National Space Agency (SANSA)
Manufacturing:	SunSpace (Satellite manufacturer)
Satellites in Orbit:	NSIGHT-1 (1998), ZA-AEROSAT (1998), SunSat (1999), SumbandilaSat (2009), ZACUBE (2013), KONDOR E (2014)
Defense and Aerospace:	Denel Dynamics (state owned company), Marcom Aeronautics
Military:	Denel Overberg Test Range (OTR) in Arniston
Initiatives:	Square Kilometer Array (SKA), Karoo Array Telescope (MeerKAT)
Legislation:	Space Affairs Act (1993), South African National Space Agency Act (2008)

Summary of Industry

South Africa's space industry has a rich history dating back to the 1950s. It has positioned itself as an "active participant in the global space arena and a country with unique space infrastructure."[83]

Threats to Industry

Brain drain has been considered a threat to the industry, and the industry has had to rely on recruiting foreign specialists. There have also been periods of decreased turnover in military expenditure impacting investment in the space domain[84]. Project Condor was the name given to a joint satellite surveillance program between Russia and South Africa in 2015. The satellite system would provide surveillance coverage of the entire African continent. South Africa did not seem to have control and oversight over the program[85].

Notable Cyber Attacks

- Cobham aircraft satellite communications equipment was the focus of research by hacker Ruben Santamarta. Ruben claims that there are vulnerabilities in Cobham's communications equipment that he discovered by reverse engineering the software[86].
- Sensitive information related to Denel was dumped when Armscor was targeted in #OpAfrica by Anonymous in 2016.[87]

[83] https://www.sansa.org.za/overview/history

[84] http://www.sansa.org.za/attachments/article/1351/National%20Space%20%20Strategy.pdf

[85] https://mg.co.za/article/2015-02-26-secret-russian-satellite-surveillance-revealed

[86] https://www.reuters.com/article/us-cybersecurity-hackers-airplanes/hacker-says-to-show-passenger-jets-at-risk-of-cyber-attack-idUSKBN0G40WQ20140804

[87] https://www.hackread.com/anonymous-hacks-south-african-arms-agency/

Transport

Represented by:	Ministry of Transport
Subsectors:	Air freight, airlines, airports, logistics, airlines, marine, road and rail
Primary Focus:	Infrastructure and provision of services for moving people and goods
Commercial Companies:	Transnet, South African Airways (SAA), SA Express (SAX)
Public Entities:	Acsa, ATNS, CBRTA, PRASA, Ports Regulator, Railway Safety Regulator, RAF, RTIA, RTMC, SACAA, SAMSA, SANRAL
Major Airports:	OR Tambo International, Cape Town International, King Shaka International, Bloemfontein International, Port Elizabeth International, Upington International, East London Airport, George Airport, Kimberley Airport

Summary of Industry

"South Africa tops the list for having the most developed transport and logistics sector in Sub-Saharan Africa."[88]

Threats to Industry

People travelling from airports have periodically been assaulted and robbed. Media reports that insiders at airports are working with thieves to identify potential victims[89]. There is also an ongoing conflict between taxi companies that has resulted in drivers getting shot. Innocent people have also been killed in the process[90].

Notable Cyber Attacks

- In June 2017, Maersk Southern Africa was infected with Petya ransomware. The infection closed down "container shipping, port and tugboat operations, oil and gas production, drilling services and oil tankers."[91]
- DSV Global Transport and Logistics in Sidwell was infected with ransomware in January 2017. DSV was able to recover the data without paying a ransom due to the data being backed up[92].
- O.R. Tambo airport, alongside more than 100 airlines globally, was impacted by Altea software suffering from a network failure. Airlines were forced to check in travelers manually[93].
- The South African National Roads Agency Limited (SANRAL) E-Toll website was hacked, making the site vulnerable to release of personal details[94]. In 2012, the E-Toll website was also the target of a denial-of service attack, but the attack was not successful[95].
- In 2015, the Road Traffic Management Corporation (RTMC) lost R 8.5 million to a series of illegal transfers by hackers[96].
- Gautrain Management Agency's bank account nearly lost R 800 million to a hack.[97]

[88] https://www.pwc.co.za/en/industries/transportation-and-logistics.html

[89] http://www.traveller24.com/News/Alerts/update-travellers-warned-to-be-vigilant-as-or-tambo-airport-spotter-crime-syndicate-probed-20170628

[90] https://www.news24.com/SouthAfrica/News/commuters-live-in-fear-over-taxi-wars-20170905

[91] http://www.ftwonline.co.za/article/123348/BREAKING-NEWS-Maersk-SA-hit-by-global-cyber-attack

[92] http://www.heraldlive.co.za/news/top-news/2017/02/04/hackers-wreak-havoc/

[93] https://www.mirror.co.uk/news/world-news/global-airport-chaos-after-computers-11251887

[94] https://mybroadband.co.za/news/security/94554-e-toll-website-flaw-a-cyber-attack-sanral.html

[95] https://www.itweb.co.za/content/VKA3WwMdwG47rydZ

[96] https://www.iol.co.za/capetimes/news/roads-agency-account-hacked-for-r85m-1928834

[97] https://www.itweb.co.za/content/gxnklOqzGX8v4Ymz

Water

Represented by:	Department of Water and Sanitation (DWA)
Sector Organizations:	South African Association of Water Utilities (SAAWU)
Infrastructure:	4,395 dams, 35,000km of pipeline, 200,000km of reticulation systems, 152 water service authorities and providers
Rivers:	Orange River, Limpopo River, Incomati River, Maputo River, Tugela River, Olifants River and Breede River
Water Boards:	Amatola Water board, Bloem Water, Botshelo Water, Bushbuckridge Water Board, Inkangala Water Board, Lepelle Northern Water, Magalies Water, Mhlathuze Water, Namakwa Water, Overberg Water, Pelladrift Water, Rand Water, Sedibeng Water, Umgeni Water
Primary Focus:	To ensure South Africans have access to clean and sanitized water
Legislation:	National Water Act, Water Service Act (1997), Municipal Systems Act

Summary of Industry

South Africa is a water scarce country with issues such as water pollution causing disease and death[98]. Approximately 70% of South Africa's GDP is dependent on the water produced from the Limpopo, Inkomati, Pangola, and Orange Rivers[99].

Threats to Industry

The country has experienced a number of years of drought, resulting in eight provinces declaring disasters and in need of drought-related intervention. It is estimated that based on current trends, the demand for water will outstrip fresh water resources by 2025[100]. Cities like Cape Town are approaching "day zero," where engineers will turn off the water to a million homes, establishing water collection points in place of piped water. There are concerns this will bring panic. The biggest reservoir (Theewaterskloof Dam), which was full four years ago, is now mostly dry. Some have pointed to climate change as a cause[101].

Notable Cyber Attacks

- Compromised passwords resulted in the National Department of Water Affairs (DWA) losing R 2.84 million in 2011.[102]

- In 2016, Anonymous Targeted the Department of Water Affairs as part of #OpAfrica and #OpMonsanto campaigns. Data was stolen and dumped online including sensitive information of government employees. They accessed the sites administrative panel, which contained information on projects and quality measurement from water supply stations[103].

[98] http://www.dwa.gov.za/documents/AnnualReports/AR%202016-17_FINAL_Inhouse_210917.pdf

[99] http://www.dwa.gov.za/IO/Docs/CMA/CMA%20GB%20Training%20Manuals/gbtrainingmanualchapter1.pdf

[100] http://www.dwa.gov.za/IO/Docs/CMA/CMA%20GB%20Training%20Manuals/gbtrainingmanualchapter1.pdf

[101] https://www.theguardian.com/cities/2018/feb/03/day-zero-cape-town-turns-off-taps

[102] http://wiredspace.wits.ac.za/bitstream/handle/10539/23573/AJIC-Issue-20-2017-Van%20Niekerk.pdf?sequence=3

[103] http://news.softpedia.com/news/anonymous-hacks-south-african-department-of-water-affairs-500412.shtml

South Africa's Cyber Defense

Between 2016 and 2017, South Africa's Department of Defense developed a "Cyber Warfare Strategy" that included intent to enhance offensive actions. The government passed a National Cybersecurity Policy Framework (NCPF) in March 2012. The "Cybersecurity Hub" is South Africa's National Computer Security Incident Response Team (CSIRT), working with stakeholders from government, private sector and civil society to counter cyber threats[104]. The DoD is seeking to establish a Cyber Warfare Command Centre Headquarters. Denel announced it will build its own cyber command center called the Denel Tactical Cyber Command Center (DTC^3)[105]. Denel said in a statement that "DTC^3 will be the cyber security operational centre for Denel…DTC^3 will also provide specialist cyber security solutions and services including a defensive and offensive cyber warfare capability"[106]. In order to help combat cybercrime, the Cybercrimes and Cyber Security bill was passed in 2016[107].

Conclusion

The critical national infrastructure of South Africa appears to be particularly vulnerable to racial tensions, drought and water shortages, social unrest, Xenophobic attacks, high crime rates, government corruption and gang violence. Of particular concern is the relationship between the nation's dependence on water and other critical industries. Electricity generated by coal is dependent on the chemical industry for processes that are heavily water dependent. Blackouts and operational failures have occurred in the past and are likely to continue. These areas are visible weaknesses in the functional well-being of the state and therefore exploitable.

The nation's levels of inequality, comparatively some of the worst in the world, have likely exacerbated the levels of societal tensions that exist along racial lines. Hacktivism has been present in some of the sectors but does not seem to be as prevalent or as popular as physical protest. Conversely, the communications and government sectors have both experienced targeting from Advanced Persistent Threats (APT) such as APT10, Careto APT, and the Equation Group under Operation Socialist (believed to be the NSA and GCHQ).

Organized crime and gang violence appears to permeate a few of the sectors. The threat of attack or robbery impacts even innocent people in the process of going to the hospital in an ambulance. These criminal conflicts are occurring in an environment which also suffers from illegal smuggling of wildlife. Although not reported on in depth, the relationship between the Yakuza and the hack on Standard Bank reveals a troubling trajectory for how the future of organized crime is likely to look.

Recent large-scale ransomware attacks (WannaCry & Petya) have exposed vulnerabilities in organizations related to critical infrastructure. The ability to defend against and recover from such attacks should be a key focus to prevent future damages and potential broad impact to the region.

There are a number of sectors that have very few companies that are responsible for large parts of supply. Some of these companies have already been investigated for exposure to cyber-attack, including Sasol and Telkom. Future research would take a deeper look at these companies to investigate how vulnerable they are to attack.

[104] https://www.cybersecurityhub.gov.za/

[105] http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=49368:department-of-defence-aims-to-beef-up-cyber-security&catid=111:sa-defence&Itemid=242

[106] http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=45119&catid=74&Itemid=30

[107] http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf