COMMUNICATIONS SURVEILLANCE BY THE SOUTH AFRICAN INTELLIGENCE SERVICES

Heidi Swart

February 2016

A report commissioned Media Policy and Democracy Project, a joint project of the Department of Journalism, Film and Television at the University of Johannesburg and the Department of Communication Science at Unisa

CONTENTS

Appendices

1. INTRODUCTION

This report was commissioned by the Media Policy and Democracy Project, a joint project of the Department of Journalism, Film and Television at the University of Johannesburg and the Department of Communication Science at the University of South Africa (Unisa). The research detailed here was undertaken to explore the South African intelligence services' capacity to intercept the private telecommunications (including packet-switched and circuit-switched communications) of the country's citizens. In particular, illegal government telecommunications interception was investigated.

The study was carried out from 1 July 2015 to 29 February 2016.

Of particular interest during this research was the government divisions that were reported to have abused telecommunications interception. These include the South African Police Service Crime Intelligence Division (CID) and the State Security Agency (SSA). With regard to the SSA, four entities within this agency were of particular interest. These included: the Domestic Branch of the SSA (Formerly known as the National Intelligence Agency and commonly still referred to by this name by former intelligence officials); the Foreign Branch of the SSA (Formerly known as the South African Secret Service and commonly still referred to by this name by former intelligence officials); the National Communication Centre (NCC), and the Office of Interception Centres (OIC).

However, these are possibly not the only government entities that utilise surveillance technology; the government entities listed below have shown interest in interception technology. Their names appeared on the list of attending organisations for the 2014 TeleStrategies convention in South Africa, an event (titled Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering) that takes place annually in the United States, South America, Europe, Africa, the Middle East and South East Asia. Below is the 2014 list of ISS attendees for the South African event:[1]

- The government of South Africa
- SA Defence Intelligence
- SA Department of Justice
- SA National Defence Force
- SA National Prosecuting Authority
- SAPS Crime Intelligence
- SAPS Forensic Division
- South Africa National Defence Force

[1] ISS World Africa 2014 Attendee Demographics. See http://www.issworldtraining.com/ISS_SA/Demo20graph14ics.pdf

- South Africa OIC Department
- South African Parliament
- South African Police Service
- South African Diamond Board
- South African National Parks
- South African Revenue Service
- South African Special Forces
- State Security Agency
- State Information Technology Agency
- Telkom South Africa

The extent to which the above organisations are involved in interception, if at all, requires further investigation.

In order to gather information for this research, several persons were interviewed on and off the record; many of them chose to remain anonymous. Interviewees included former intelligence officials and various professionals working in the private security sector with intimate knowledge of the inner workings of the government's intelligence services. A list of sources is provided in Appendix A.

Information from product brochures for interception equipment was incorporated into the study and newspaper reports on surveillance issues in South Africa and abroad were reviewed.

The report contains findings about four different interception technologies, including bulk interception technology, handover interfaces utilised by telecommunications service providers, IMSI catchers and cyber surveillance tools.

Finally, recommendations are made for further investigations.

2. THE CAPACITY OF SOUTH AFRICAN STATE INTELLIGENCE SERVICES TO INTERCEPT TELECOMMUNICATIONS

For the purposes of this research, telecommunications interception was taken to include the interception of data communications (communicated via mobile communications and fixed-line networks), voice communications (communicated via landline or mobile networks) and metadata (also known as call-related data, which includes the time of call, duration of call, caller identity, receiver identity and location of the caller and receiver).

Interception can be categorised according to the number of persons targeted simultaneously. To this end, a distinction is made between targeted interception, on the one hand, and bulk interception (also known as mass interception, blanket interception, or massive, passive interception) on the other.

Targeted interception refers to the monitoring of specific individuals or groups of individuals, usually for a set period. Bulk interception is ongoing monitoring, recording and storing of the communications of large sections of the population. With bulk interceptions, millions of people's communications can be recorded simultaneously.

The South African government is known to possess equipment to carry out both types of interception.

2 .1 South Africa's Bulk Interception Capacity

South Africa's bulk interception facilities are controlled by the SSA and located at the NCC in Pretoria. The NCC focuses on the interception of foreign signal intelligence interception. This type of interception is applicable to communication that originates in, passes through or terminates within the borders of South Africa. There are no laws regulating the NCC or foreign signal interception in South Africa. The only laws governing any communications signal interception in South Africa is the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (Rica). However, this law only applies to domestic signal interception. Intercepting communications between two persons in South Africa, where they have not agreed to the interception, is illegal unless it is approved by a judge in terms of Rica. However, with the NCC unregulated, and given the limitations of Rica, the privacy of communications through services such as Gmail, where servers are located outside South Africa, are not protected by any laws (even if both the sender and the receiver are in South Africa). In 2013, despite various voices in civil society pointing out the unlawful and unconstitutional nature of the NCC's operations (given that they are not legally regulated), the General Intelligence Laws Amendment Bill was signed into law without so much as mentioning the NCC. The bill had presented an opportunity for government to establish

legal regulations to govern the NCC, yet no steps were taken to do so. [2] [3] [4] [5] [6]

The bulk interception facilities at the NCC have been used in the past to spy on citizens illegally for political reasons. In 2005, the Inspector General of Intelligence (IGI), a government entity tasked with the oversight of intelligence services, found that at least 13 people's telecommunications had been intercepted illegally using the NCC's mass interception facilities. An investigation into the illegal interception at the NCC was initiated after Saki Macozoma, then a member of the National Executive Committee, lodged a complaint with Ronnie Kasrils, the Minister of Intelligence at the time. [7]

In order to further investigate South Africa's capabilities to intercept telecommunications en masse, various interviews were held with anonymous sources. News reports and surveillance technology product brochures were reviewed. Of particular interest was VASTech SA Pty (Ltd) (hereinafter referred to as VASTech), since VASTech is South Africa's leading producer of mass interception technology and have repeatedly been connected to the South African government.

Three independent sources who spoke off the record alleged that bulk interception was occurring in South Africa.

According to SOURCE A – a person with close connections to the private sector producing mass interception technology locally, who has personal contact with the top management of VASTech – bulk interception has been occurring for the past decade in South Africa. SOURCE A alleged that the government agencies could look up the past conversations of any citizen and that these communications were stored for years. SOURCE A did not go into detail, but alleged that this was how Zuma escaped his corruption charges. SOURCE A also did not provide detail about which government agencies were involved in this mass interception. The source could not provide details about the exact technology utilised by the state. The source neither confirmed nor denied that VASTech's technology was used by the state to carry out bulk interception.

SOURCE B, who has close ties with a technician directly involved in equipping the government with mass surveillance capacity, said that the SSA had been intercepting *all* citizens' communications for

---

[2] Ad Hoc Committee on General Intelligence Laws Amendment Bill (NCOP), General Intelligence Laws Amendment Bill: State Security Agency briefing, 15 May 2013.
See https://pmg.org.za/committee-meeting/15852/

[3] L. Nathan, 'A critique of the General Intelligence Laws Amendment Bill', Politicsweb, 19 April 2012.
See http://www.politicsweb.co.za/documents/a-critique-of-the-general-intelligence-laws-amendm

[4] K. Rice, ' Spy bill passed', Tech4Law, 17 June 2013
See http://www.tech4law.co.za/business4law/efficient-business-process/spy-bill-passed.html

[5] Ministerial review commission on intelligence, 'Intelligence in a constitutional democracy: Final report to the minister for intelligence services', 10 September 2008
See http://www.r2k.org.za/2013/02/11/matthews-commission-gilab-south-africa-spies/

[6] Privacy International, **'The Right to Privacy in South Africa', Submission in the advancement of the consideration of the periodic report of South Africa, Human Rights Committee, 116th Session, 7 – 31 March 2016.** See https://www.privacyinternational.org/sites/default/files/HRC_SouthAfrica_0.pdf

[7] Office of the inspector general of intelligence, media briefing, 23 March 2006.
See http://www.oigi.gov.za/Speeches/IG%20Exec%20Summary%2023%20Mar%2006.doc

at least the past five years.

> The public is completely unprotected. Every call of every cell phone, every call from every landline is channelled electronically. In the past, this was only done with calls that went out to foreign countries. Now it is every call. Millions per day. It is channelled and stored in Pretoria. It sounds like a fairy tale: unbelievable. And that is the problem in this terrain.

The source added that all metadata and data communications were also intercepted en masse. Thus all packet- and circuit-switched data is targeted.

SOURCE - a former military intelligence operative with inside knowledge of the workings of the NCC – stated that to his knowledge the NCC's bulk communications facilities had been used in the past to intercept the conversations of the Hawks, various South African banks and government officials.

None of the above sources could provide details about the exact brand of technology used, the manufacturers or the distributors.

It is worth noting that during the course of this research project – which looked not only at mass interception, but also at the use of IMSI catchers, the targeted use of service provider handover interfaces and cyber surveillance technology – these three sources were the only ones of 11 interviewees who showed any knowledge of mass interception technology being used in South Africa. One highly esteemed cybercrime investigator, who is in private practice, made the argument that mass interception was not possible because there was simply too much data to capture. Of all the interception technologies, mass interception appears to be the least understood; even within the intelligence community itself.

VASTech SA (Pty) Ltd

Although sources could not confirm the specific technology in possession of the South African government, it is well known that a South African company, VASTech, is both an established producer of mass interception technology and a company that has enjoyed financial support from South Africa's Department of Trade and Industry. It has been reported to have concluded at least one business contract with the South African government. This study revealed additional connections between VASTech and the South African government.

VASTech's products

The following is a brief summary of VASTech's products, based on product brochures released by Wikileaks in 2011.[8] [9]

[8] VASTech presentation, 'Passive surveillance in support of LI', October 2008. See https://www.wikileaks.org/spy-files/docs/vastech/41_passive-surveillance-in-support-of-li.html

[9] VASTech company overview, October 2011. See https://www.wikileaks.org/spyfiles/docs/vastech/182_vastech-company-overview-communication-intelligence.html

The Zebra

The Zebra is a network interface that simultaneously monitors and records millions of voice calls, SMSes, MMSes, emails and faxes in the networks to which it is connected. It also captures the metadata of these communications: when the communication took place, the duration thereof and which parties were involved. It can be connected to landline networks and mobile networks. The Zebra stores this information online for 'extended periods of time', although the available brochures do not specify exactly how much information can be stored and for how long. Information is stored in an online database that is scalable. The Zebra also allows for analysis of stored information. It allows law enforcement officers to 'go back in time' to find relationships between people based on their conversations and to identify new suspects: 'It allows the investigator to identify targets and discern relationships which may have their origins years into the past'.

The Badger

The Badger is an interface focused on mass interception of internet traffic; broadband networks in particular. It is used to monitor internet activity, including internet downloads, social media, web-based email services, VoIP and browser activity.

The Satellite Signal Analyser

When the Zebra and the Badger are used in conjunction with the Satellite Signal Analyser, satellite communications can also be intercepted, stored indefinitely and analysed.

If the three products are utilised together, all forms of communications on fixed-line networks, mobile networks and satellite networks can be monitored. This includes communications within a country's borders, across borders and spanning the globe. When a cell phone is in roaming mode, the system can still track its data and call communications.

One aspect of the system which is used as a selling point is that it is a passive monitoring system, meaning that it quietly records communications without interfering with the network. This allows 'independence from the operator personnel, thereby allowing independent operation for the security agency'. In other words, law enforcement can monitor without the knowledge of the network operator.

Another feature of the Zebra is that it allows for the prediction of crime because it can monitor the activities of suspects in detail and over long periods. However, current legal processes, as described in Rica, call for law enforcement to first have sufficient evidence before a suspect's communications can be intercepted and that interception should be a last resort. With passive monitoring, the opposite occurs: individuals' communications, whether these individuals are suspects or not, can be intercepted from the get-go. In South Africa, this approach to intercepting communications is illegal.

VASTech's connection to the South African government

VASTech, with offices in Stellenbosch, Somerset-West, Pretoria and Dubai, primarily supplies mass surveillance equipment to Africa, Asia and the Middle East. Founded in 1999 by Frans Dreyer, who died in a 2011 plane crash in Libya, VASTech's turnover was over R30 million by 2006. It was reported in 2006 by iWeek that the company 'concluded a significant three-year contract for a recording solution with the SA government' in 2005."[10] [11] The company has a history of connections with South African government entities.

Council for Scientific and Industrial Research (CSIR)

The CSIR is a National Government Business Enterprise and government funding is a crucial income source for the organisation. When asked how long VASTech had been renting premises from the CSIR, the Institute stated that the company has been a tenant at the CSIR Scientia Campus in Pretoria since 1 February 2005.

It would not be unusual for the institution to undertake support of such a project.

According to the CSIR's website,

> The CSIR's role as national defence science, engineering and technology (SET) capability is integral to the country's security. The CSIR is recognised by the national Department of Defence and others in the defence domain as a prime R&D agency and operates as its strategic 'in-house' science and technology defence capability in many areas.
>
> On the whole, providing our armed forces with the ability to detect threats, secure borders and protect the lives within, is the substance we offer the defence and security of South Africa and its people. [12]

A former crime intelligence police official with particular knowledge of cyber surveillance (SOURCE F) said that VASTech is the type of project that the CSIR would back and that it was not unusual for the CSIR to team up with the private sector.

> The CSIR is big on that type of research. A company I used to work for were offered offices at the CSIR; the CSIR wanted to do a joint project with them …

However, the CSIR said that its relationship with VASTech was limited to office rental. When questioned, it was stated that 'the CSIR is not involved in the development of interception technology or any other technology with VASTech SA (Pty) Ltd. The organisation has not contracted or partnered with VASTech and such technology was not developed through a CSIR project' (See Appendix B).

[10] Insider Surveillance, 'South Africa's VASTech: Surveillance Leader of the Developing World', 8 January 2015.

[11] iWeek, 'Intelligence Gatherer', 27 April 2006. See http://www.iweek.co.za/leadership/intelligence-gatherer

[12] CSIR website, December 2015. See http://defsec.csir.co.za

The Innovation Hub

The Innovation Hub was founded in 2001 by the Gauteng Provincial Government to drive local innovation in several sectors, including information and communication technology. The Innovation Hub was part of one of the 'mega projects', which the Gauteng Provincial Government earmarked for investment through its multibillion rand initiative, BLUE IQ. The Hub was intended to serve as premises for start-up companies from the CSIR and the University of Pretoria.[13] [14]

By 2006, VASTech 'graduated' from the Innovation Hub's 'incubation' programme for small to medium enterprises, known as the Maxum Business Incubator. The Incubator supports and thereby fast-tracks start-ups, providing resources like office space, legal services, intellectual property support, marketing and financial assistance, including debt financing from banks and equity financing from venture capitalist.[15]

The Innovation Hub responded to questions regarding their involvement with VASTech as follows:

> VASTech was incubated at Maxum Business Incubator during the pilot operation at the CSIR, and left incubation in 2006 and they are now operating from the Stellenbosch technology park. VASTech was never funded by Maxum, we do not fund entrepreneurs. As a start-up company, VASTech was offered space to operate and business mentorship. The Innovation Hub was aware of the product and services that VASTech was developing while they were incubated. Their activities and clients were legal. As a government agency, it is our policy to support technology start-up companies and promote their growth in the market (See Appendix C).

The Department of Trade and Industry

The Department of Trade and Industry has funded VASTech on two occasions after this. In the 2007/2008 financial year, the DTI had approved a grant of R1.3 million to the company for its development of the Zebra, and in 2010 it approved an additional grant for R2.69 million to fund project 'NEXT', the details of which are as yet unknown.[16] [17]

In November 2013, the DTI told the Mail & Guardian newspaper that the department was aware that VASTech's technology would be used for bulk interception and based on VASTech's funding proposal, believed it would be employed to monitor 'Borders and Stadiums, among other things'. The DTI funding of VASTech came under scrutiny when the Wall Street Journal reported in 2011 that the VASTech Zebra was found in a surveillance centre of Gadhafi's forces in Libya and was used to spy on private citizens. VASTech never denied the allegations and stated that it sold its equipment

---

[13] City of Johannesburg website, December 2016. See http://joburg.org.za/index.php?option=com_content&task=view&id=993&Itemid=58

[14] CSIR media release, 'CSIR and The Innovation Hub to strengthen innovation in Gauteng', 20 March 2013. See http://ntww1.csir.co.za/plsql/ptl0002/PTL0002_PGE157_MEDIA_REL?MEDIA_RELEASE_NO=7525753

[15] The Innovation Hub, media release, 'Business incubation is boosting SME development', 18 April 2006. See http://www.itweb.co.za/office/theinnovationhub/PressRelease.php?StoryID=161445#author

[16] Annual Report of the Department of Trade and Industry Support Programme for Industrial Innovation, 2008. See http://www.spii.co.za/content/Annual%20Reports/SPII_Annual_Report_2008.pdf

[17] Annual Report of the Department of Trade and Industry Support Programme for Industrial Innovation, 2010. See http://www.spii.co.za/content/Annual%20Reports/SPII_Annual_Report_2010.pdf

to governments that were not on the United Nations' arms embargo list. The DTI said that when it funded VASTech's development of the Zebra, it did not know that it would be used for 'nefarious activities'.[18] [19]

Al-Jazeera Spy Cables

Further insight is provided into VASTech's relationship with the government by the so-called Spy Cables – top secret intelligence documents from various governments that were leaked to Al Jazeera in February 2015. One such leaked document from South Africa's National Intelligence Agency (NIA) – today the Domestic Branch of the State Security Agency – was titled 'Operational Target Analysis: Iran'. Dated January 2010, the document details how the Iranian government delegation visited the National Communications Centre in May 2005. The NCC reported that the Iranians were particularly interested in interception technology, including data recording and 'passive GSM monitoring', the latter referring to the monitoring of mobile networks. Both of these are focus areas of VASTech. The Iranian delegation then paid a visit to VASTech where they were provided with information about 'active lawful interception' and 'passive unrestricted monitoring'. Further on in the document, the NIA expresses concerns that VASTech – along with entities like DENEL (a commercial enterprise owned by the South African government that designs weapons technology), the CSIR, the NCC, the South African Secret Service and the National Intelligence Agency itself – could be targeted by the Iranian intelligence services. [20]

Despite VASTech's interactions with the South African government, no proof has emerged confirming that the state's intelligence services are using VASTech's equipment. However, in an interview with VASTech founder Frans Dreyer, published by iWeek in 2006, it was stated that VASTech had at the time signed a three-year contract with the South African government to provide them with a 'recording solution'. No mention is made of the specific product or government department involved in the contract or of the details of the technology. [21]

VASTech in the International Arena

Middle Eastern governments are a major part of VASTech's target market. To better understand the South African government's relationship with VASTech, an interview was held with Sam Vaknin, a seasoned reporter in the Middle East and the Balkans, with sources linked to Israeli and other intelligence agencies.

---

[18] *Mail & Guardian*, 'DTI 'funded Gaddafi spyware', 22 November 2013. See http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware

[19] The Wall Street Journal. Firms Aided Libyan Spies, 30 August 2011. See http://www.wsj.com/articles/SB10001424053111904199404576538721260166388

[20] National Intelligence Agency, 'Operational Target Analysis: Iran', January 2010. See https://assets.documentcloud.org/documents/1672715/south-africa-operational-target-analysis-of-iran.pdf

[21] iWeek, 'Intelligence Gatherer', 27 April 2006. See http://www.iweek.co.za/leadership/intelligence-gatherer

Vaknin said that the Zebra did not fit South Africa's intelligence profile and that he understood South African intelligence services preferred targeted interception to mass interception.

> It would be journalists, liberal activists, academics, enemies of intelligence services. This equipment (like the Zebra) is truly all-pervasive. It's for countries who want to monitor literally every single phone call, every single sms, every single email and IP, and Voice Over IP conversation. With minimal investment – a tiny room, toilet size – you can have equipment that could listen in on twenty million people. South Africa is not this kind of country – whatever you may think of the government. South African authorities and intelligence services are definitely widely tipped to be abusing surveillance for their own ends. But they are far more likely to use malware injectors, and software like FinFisher or FinSpy.

Expanding on his understanding of VASTech's relationship to the South African Government, Vaknin said there were rumours within global intelligence circles that the South African government initially collaborated with the Russian intelligence agencies (including the Federal Agency for Government Communications and Information and the Federal Security Service) to fund VASTech.

> Each government pledged to purchase at least one system as a form of financial support. The SA services are using the Zebra only spottily and sporadically. The Russians ordered two or three additional systems over the years and gave them to allies.

Vaknin said that, after VASTech's founder, Frans Dreyer, died in a plane crash in Libya in 2011, VASTech's ties with the South African government strengthened.

> What is absolutely sure is that after the founder died in this plane crash, VASTech was in panic, and everyone thought it was about to die. Then they hopped into bed with the government much more forwardly. And they are considered government in global intelligence circles. People talk about them as if they are the long arm of South African government. No one will regard them as private sector.

VASTech is a major role player in the international market for surveillance equipment (particularly in Africa and the Middle East) and is linked to the South African government. At the very least, it can be stated with certainty that the South African government has access to VASTech's technology and it is certainly within the government's means to purchase the technology that it helped to develop. The government's expenditure of tax payers' money on VASTech's development as a company and on its actual products requires further investigation, as does the extent to which the SSA employs VASTech technology, if at all.

2.2 The Use of IMSI (International Mobile Subscriber Identity) Catchers

The IMSI (international mobile subscriber identity) catcher (also known as a 'grabber' or 'stingray') is a portable piece of equipment, consisting of a laptop computer, one or more antennae and a compact base station the size of a shoebox or a desktop computer tower, depending on the make and model. This is a mobile device designed for close-range monitoring of a subject – within a few 100 metres to as much as 10km and more, depending on how advanced the specific model is.

The functioning of IMSI catchers

An international mobile subscriber identity (IMSI) number is contained in the mobile phone's Sim card. Each subscriber to a network service provider has a unique IMSI assigned to his or her Sim card. Thus, in South Africa, since the IMSI is linked to a Sim card, and a Sim card is registered in a specific individual's name, the IMSI can be used to identify a specific target – granted that the Sim registration is accurate and lawful. Law enforcement agencies may use the IMSI catcher in cases where mobile surveillance of criminals on the move is required.

The IMSI catcher acts as a false cell phone tower and base station. The IMSI catcher emits a stronger signal than the actual network cell phone tower to which mobile phones within that specific cell would normally connect. However, the cell phone signal is relayed from the IMSI catcher back to the actual mobile network; neither the subscriber nor the service provider will be aware that the IMSI catcher is at work.

Once a mobile phone connects to an IMSI catcher, the device in effect takes over the cell phone and switches off the encryption of the phone. This allows for access to content and metadata. The majority of smartphones do not indicate to the user whether or not encryption is turned on or off. In addition, activating encryption is handled by the network, and not the mobile phone. This means the subscriber cannot decide whether or not to turn the encryption on or off. After decryption, communications content and metadata can be freely intercepted.

IMSI catchers have varying capabilities: at the most basic level, the IMSI catcher can detect a subscriber's location within a radius of a few hundred metres. Some versions of the device can monitor the conversations, SMSes, internet communications and messenger services, such as WhatsApp, of a single phone. Still others can intercept and store thousands of mobile phones' communications simultaneously. An IMSI catcher may also have the ability to scramble cell phone signals within its range.

A product brochure of the company Verint that advertises the capabilities of the 'Engage off-air intelligence solution', states that their Engage PI2 model has the following capabilities: [22]

- To identify potential targets and build an intelligence picture over cellular networks;
- To passively and covertly collect cellular traffic in an area and analyse it in real time to identify potential targets;
- To collect mass GSM traffic over a wide area;
- To identify suspicious communication patterns using a range of analysis tools:
    - Location
    - Speech Recognition
    - Link Analysis

[22] Verint product brochure. See https://assets.documentcloud.org/documents/885760/1278-verint-product-list-engage-gi2-engage-pi2.pdf

- Text Matching
- Interception of voice calls and text messages of potential targets
- Decryption of A5/1 and A5/2 encryptions with an embedded decipher
- Operation undetected, leaving no electromagnetic signature
- Selective downgrade of UMTS traffic to GSM
- Ability of multiple users to analyse calls at the same time

Although the device can be utilised for targeted interception, it appears to be increasingly viewed as a mass interception device, because advances in technology have made it possible for such devices to intercept thousands of subscribers' communications simultaneously.

IMSI catchers in the international context

The IMSI catcher has drawn media attention internationally over the past years. The Wall Street Journal reported in 2014 that the U.S. Marshals Services had utilised IMSI catchers to collect data from thousands of mobile phones. The newspaper reported that IMSI catchers produced by Digital Receiver Technology and known as 'dirtboxes' were placed aboard five Cessna airplanes that have scoured the entire United States since 2007, indiscriminately recording cell phone communications from thousands of people across the country.[23]

In 2011, the Guardian reported that, to the dismay of civil liberty advocates, London's Metropolitan Police Service had purchased at least one IMSI catcher, said to be capable of intercepting cell phone signals in an area as large as 10 square kilometres and able to 'catch' hundreds of IMSI numbers simultaneously and allowing for real-time tracking of targets.[24]

In June 2015, Sky News reportedly found over 20 instances in which IMSI catchers were active in London over a three-week period. The news agency said that they had detected the IMSI catcher signals with the help of the security company, GMSK Cryptophone. Sky News could not establish whether or not these IMSI catchers belonged to law enforcement agencies or criminals, and neither the Metropolitan Police Service nor the British National Crime Agency would provide further details, their motivation being that they did not want to compromise their operations by discussing them in the press.[25]

In December 2014, Norwegian publication *Aftenposten* reported that, with the assistance of two private security companies, it had located no fewer than six IMSI catchers in Oslo within range of

[23] The Wall Street Journal, 'Americans' Cellphones Targeted in Secret U.S. Spy Program', 13 November 2014. See http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533

[24] *The Guardian*, 'Met police using surveillance system to monitor mobile phones', 30 October 2011. See http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance

[25] Sky News, 'Fake Mobile Phone Towers Operating In The UK', 10 June 2015. See http://news.sky.com/story/1499258/fake-mobile-phone-towers-ope'rating-in-the-uk

parliament and other government branches.[26]

Thus, globally, there appears to be a concern about the threat that IMSI catchers pose to citizens' privacy, largely because they can be employed without the knowledge of the service provider or the mobile user and because they can, if advanced enough, collect vast amounts of communications data from persons who, by chance, are close to the suspect being targeted.

IMSI catchers in South Africa

This research made an attempt to establish the capacity of the South African intelligence services in terms of IMSI catchers and the extent to which the technology is used illegally.

Sources were primarily able to comment about IMSI catchers used by police crime intelligence. However, the former crime intelligence police official and undercover operative (SOURCE E) stated that IMSI catchers were used by police crime intelligence and the branches of the SSA (foreign and domestic).

Capacity of the state in terms of IMSI catcher

A cyber crime investigator with links to intelligence services (SOURCE H) said that the Police Crime Intelligence Division had about one IMSI catcher per province. However, SOURCE H said that the features of these IMSI catchers were limited – they could only be used to locate a suspect through tracking their cell phone.

An expert in mobile security (SOURCE J), who has inside knowledge of security processes of mobile service providers, said that police had no more than four IMSI catchers nationwide, and that, as stated by SOURCE H, the capability of IMSI catchers was limited to locating a suspect through tracking the whereabouts of a cell phone.

According to a former crime intelligence police official and undercover operative (SOURCE E), the police crime intelligence division's office in Pretoria had at least three IMSI catchers in 2010. SOURCE E did not know if the division had either purchased additional IMSI catchers or decommissioned any of the devices since that time. SOURCE E said that one IMSI catcher was purchased in 2001 and the other two circa 2005. At the time, said the source, a single device cost 'millions', although the source could not provide specific amounts. Regarding the capacity of the IMSI catchers, SOURCE E stated that at least one of the IMSI catchers at police crime intelligence in Pretoria could be used to locate a target's position through his or her mobile device, listen in on a single cell phone call at a time and intercept that cell phone's SMSes and manipulate them. The caller and receiver would be unaware of the manipulation, as would the service provider.

[26] *Aftenposten*, 'Secret Surveillance of Norway's Leaders Detected', 13 December 2014. See http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html

> They have three of those things there (at police crime intelligence). All the agencies use it. The grabber, if they have my cell phone number and they want to find me, they put my number into the grabber. But my phone has to be on. Then it brings you to the spot where you are, in real-time. And then they can act on that spot. If they don't want to act, don't want to arrest you or something, they can sit there at that moment and they can… if I, say, send a message on WhatsApp or SMS or anything, then they grab your message and they can manipulate it. So, if I send a message that says, 'Hello John', they are able to intercept that message and change it to say, something like 'Bugger off, John!'. And they send it to the guy on the other side. And the guy on the other side, he receives my message from my number as if I sent that message. So that's how they can manipulate. If they are close to you then they can do anything, it's as if Vodacom is listening to your stuff live. It's like a tower; a mobile tower. A grabber can only handle one number at a time. Well, the stuff I know about could only handle one number at a time. This was up to about five years back. They bought the one in 2001 and I think the other two in 2004 or 2005, and two of them were in Navarra bakkies and the other one in a van. It's not a big machine. It looks like two of those boxes [he is referring to personal computers] next to each other, and then it has two or three screens on which you can work, with cables. Then the people sit physically on that computer and work.

It would appear that the IMSI catchers utilised by police crime intelligence are limited in number and not capable of bulk interception. If misuse does occur, it is likely to be sporadic and would probably not happen on a large scale. Although one source confirmed that all agencies used IMSI catchers, more information is required regarding the SSA's use of these devices.

Illegal private use of IMSI catchers by intelligence services

During this investigation, allegations came to light that certain police crime intelligence officials were possibly either illegally selling IMSI catchers or utilising the devices in their private capacities to earn extra cash.

According to SOURCE E – the crime intelligence official – one of the three IMSI catchers at police crime intelligence was rumoured to have disappeared.

> Five years ago, they still had three. One supposedly went 'missing' – supposedly. Under the auspices of Mr. X. He let one slip. X embezzled one. And we don't know for what purposes he embezzled that one. But that was the rumour at that time.

SOURCE G, a former crime intelligence official, with experience in processing intercepted communications within the police crime intelligence division, said that the sale of equipment by police crime intelligence members into the private sector was a distinct possibility. The source could not confirm a specific incident of an IMSI catcher being sold illegally by members of crime intelligence.

> It can happen. Where there is smoke, there's a fire. Equipment was purchased that was not on the books. But you are going to have a hard time proving it.

The source previously involved with diverse state security aspects (SOURCE B) alleged that there was an incident where police crime intelligence officials had stolen an IMSI catcher and utilised it in their private detective work. The source did not specify the time of the incident. The source claimed that a vehicle containing an IMSI catcher had been in an accident and that the officials involved seized the opportunity to claim that the IMSI catcher was damaged to the extent that it could no

longer be utilised. After this, the officers used it in their private investigations.

The private use of IMSI catchers by police officials came to light in the media in 2015, when Paul Scheepers, a police crime intelligence officer, was arrested on 8 May 2015 and appeared in court on charges of fraud and perjury, among others. At the time, the Hawks (the police's special investigative unit) were investigating Scheepers to establish if he had utilised the IMSI for private work.[27]

Almost immediately following Scheepers' arrest, the Joint Standing Committee on Intelligence – the parliamentary watchdog responsible for overseeing the intelligence services – issued the following statement on Friday, 20 November 2015:[28]

> We note as the Joint Standing Committee on Intelligence (JSCI) the suspension of Mr. Paul Scheepers, a member of Crime Intelligence. We appreciate that the matter is sub judice. We nevertheless as the JSCI, welcome the police investigations into how Mr. Scheepers came into possession of a grabber as the relevant legislation of both the Electronic Act and the Regulation of Interception of Communications and Provision of Communication-Related Information Act (Rica) is of relevance. The Committee would revisit the Rica with a view of whether any changes would be required to strengthen the Act in the likely event that the Judge is not sufficiently empowered to deal with matters such as grabbers. Of concern to us would be whether at all a member of the Crime Intelligence Unit might have been moonlighting without permission to conduct matters of crime intelligence.
>
> The JSCI will have to reflect and be guided by, among other things but in particular, the National Strategic Intelligence Act 39 of 1994, section 2, sub-section 3, which deals with the function of the South African Police Service Act. The JSCI will deliberate and take into consideration Section 3 of the Oversight Act to deliberate upon, hold hearings, subpoena witnesses and make recommendations on any aspect relating to intelligence and national security, including administration and financial expenditure.

This was the first time that the JSCI has made mention of revising Rica with regard to the regulation of the use IMSI catchers.

Laws governing the legal use of IMSI catchers by law enforcement agencies

Although the JSCI appears to be under the impression that use of IMSI catchers by law enforcement agencies is regulated by Rica, it would seem that the SSA does not view the use of these devices as being regulated by the act. In an article by Prof Jane Duncan of the University of Johannesburg that appeared in the Mail & Guardian in September 2015, the Ministry of State Security's spokesperson, Brian Dube, was asked by Duncan whether or not the SSA would apply for an interception direction in terms of Rica prior to the use of the IMSI catcher for law enforcement purposes. In his response, Dube appeared to imply that the IMSI catcher was viewed by the SSA as a mass interception device, and therefore not regulated by Rica[29]:

---

[27] IOL, 'Zille's spook had grabber', 20 November 2015. See http://www.iol.co.za/news/crime-courts/zilles-spook-had-grabber-1948290

[28] Joint Standing Committee on Intelligence media release, 'JSCI notes suspension of Mr. Paul Scheepers', 20 November 2015. See http://www.parliament.gov.za/live/content.php?Item_ID=8495

[29] J. Duncan, 'Spies are all set to grab your metadata', 11 September 2015. See http://mg.co.za/article/2015-09-10-spies-are-all-set-to-grab-your-metadata

> On the matter of procedure, the interceptions protocol applies whenever an individual's communications are to be intercepted. Such a protocol doesn't provide for mass interception as the interception judge must hear each case on its merit.

Asked if intelligence services ever obtained a court order to utilise IMSI catchers for official police purposes, SOURCE E responded in an amused tone:

> No! No. That stuff is all illegal … All of it! Where are you going to find a judge who you can convince to quickly approve the thing for you on a 12-hour basis, in a place like Newcastle or Estcourt? That is why that Indian that they flew to Pakistan…that stuff was all done live, with the grabber. [NOTE: The source is referring to Khalid Rashid who was illegally deported from South Africa in 2005, and is actually a Pakistani national.]

An expert in mobile security with inside knowledge of security processes of mobile service providers (SOURCE J) also stated in no uncertain terms that the mobile network operators did not receive court orders for the use of grabbers.

> Mobile network operators have nothing to do with the grabbers.

The source previously involved with diverse state security aspects (SOURCE B) also stated that absolutely no legal processes were followed by law enforcement when using IMSI catchers and that mobile network operators were not informed.

IMSI catchers and illegal renditions

SOURCE E provided some insight into the clandestine use of IMSI catchers by law enforcement during official procedures.

SOURCE E stated that an IMSI catcher had been used in the illegal rendition of Pakistani national, Khalid Rashid in 2005. The source said that on the night of 31 October 2005 Rashid was located by a task team of intelligence forces at a private home in Estcourt, KwaZulu-Natal, through the use of an IMSI catcher.

According to Rashid's attorney, Yasmin Omar, witnesses reported that police forcefully entered the home by breaking down the front door and they flung furniture around inside the house. Rashid was taken away as family and friends looked on. He was first taken 450km away to the Cullinan police station in Gauteng and detained. On the evening of 6 November he was flown out of the country on an unscheduled flight. Two years later, Rashid told Omar (the two have, to this day, never met in person) that his whereabouts had been unknown to him as he had been hooded while flown from one location to the other. This continued for the better part of two years.

Omar said that shortly after Rashid was taken from South Africa, he was flown to an unknown port of entry in Kenya.

> From Kenya, we are not certain; at that stage investigations suggested that he may have been taken to the Channel Islands. Others suggested he was taken to Guantanamo. He was tortured extensively, he was waterboarded, he was incarcerated; they put on a light continuously so that he wouldn't fall asleep.

Rashid was released and taken back to his hometown, the city of Lahore in Pakistan, about two years after his deportation. Omar said that this only happened after Amnesty International threatened to go to the International Criminal Court and also threatened that steps would be taken to arrest the president of Pakistan and various other officials attached to Pakistani and South African intelligence services.

In 2009, South Africa's Supreme Court of Appeal ruled Rashid's detention and deportation unlawful because a warrant had not been obtained in terms of the Immigration Act 13 of 2002. Rashid came from Pakistan to South Africa 'a few months' prior to his deportation, according to court documentation. The court did, however, rule his arrest to be lawful, since it found that he was an illegal foreigner. [30]

However, SOURCE E contends that Rashid was in fact a Pakistani agent and that the reason for his detainment at the Cullinan police station was for South African intelligence to question him on intelligence matters. SOURCE E said that he was not harmed in any way by South African intelligence forces.

> After they (the Police Crime Intelligence Division) found him (Rashid), they let the Pakistanis know, because he had completely disappeared off the radar. The Pakistanis did not know where to find him. When they did find him, they let the Pakistani intelligence know, 'Listen, we've got the guy, we're positive it's him,' and from there they went immediately with one of their planes, or, I don't know what plane, if it was the Pakistani plane, but it was a Boeing 727, they flew to South Africa, landed at Waterkloof. From Cullinan he was taken to Waterkloof. Late night he was handed over to the Pakistanis, and in a very friendly, comfortable condition (sic). In the meanwhile the plane was refuelled, and just after the man was in, the airplane departed and he was gone. The Pakistanis then kept him off the record for about two years, and now he was, about a year and a half, two years ago, he surfaced again in some country; he was reported as dead or missing, but now he's back in the raghead's activity. It was all a cover operation for the ragheads – he was part of them all along. He was actually working for intelligence, the Pakistani intelligence. Although the Americans and the Pakistanis have an agreement with each other, they wanted to bring this guy to book anyway because he aided Al Qaeda during the 9/11 attacks.

SOURCE E further stated that a second Pakistani national, Altaaf Kavi* [name unclear on audio], was an example of a similar case and that he was also located with an IMSI catcher before being sent out of South Africa.

> He, in accordance with the British MI6…MI6 paid for everything. Everything. He was picked up with the grabber and he went to Palestine, no, um…I don't remember the name of the country. The British paid for everything. The airplane, they even paid for the airplane here and he was taken to that country. If I remember the country I will let you know. And they wanted to question him there first, and then the British could question him further, on the condition that he may not be handed over to the Americans. He was definitely a terrorist.

[30] Supreme Court of Appeals, media release, 'Ismail Ebrahim Jeebhai & others v Minister of Home Affairs & another', 31 March 2009. See http://www.saflii.org/za/cases/ZASCA/2009/35media.pdf

Illegal use of IMSI catchers by civilians

Aside from IMSI catcher*s* used by South African law enforcement, there have been reports of these devices being used for private gain by civilians. Private ownership of such a device is illegal in South Africa.

On 31 July 2015, Independent Media reported that two men were arrested at the Irene Village Mall in Centurion for the possession of an IMSI catcher. Independent also reported that state intelligence officials were looking for two other IMSI catchers that were in the hands of private individuals. Sources told The Star newspaper (part of the Independent Media group) that authorities were concerned that the IMSI catcher would be used to help a 'syndicate win billions in government tenders and compromise national security'. The newspaper stated that an intelligence operative, who wished to remain anonymous, informed the paper that the IMSI catcher posed a 'serious security threat. Only certain people are authorised to use this machine. No ordinary citizen is supposed to be in possession of this device'. The article also stated that the IMSI catcher was an Israeli model.[31]

The *Cape Times* newspaper (part of the Independent Media group) further reported on 27 August 2015 that the Hawks were searching for two IMSI catchers that had fallen into private hands and that the device, according to an anonymous source, allegedly had the ability to intercept voice calls.[32]

However, SOURCE H (a cyber crime investigator with links to intelligence services) asserted that there were as many as six IMSI catcher*s* in private hands. SOURCE H added that these were usually used illegally by, for example, moneylenders to locate evasive debtors and that they were brought into the country illegally and not through law enforcement channels. SOURCE H explained that an IMSI catcher can, for example, be brought into the country piece by piece and reassembled once all the parts reach South Africa. SOURCE H referred specifically to the IMSI catcher seized in the Irene Mall in Pretoria, stating that a company by the name of Verint (mentioned above) was responsible for importing that device in this manner.

This is in accordance with what sources told Independent Media about the IMSI catcher seized at the Irene Mall: The Cape Times was told by an anonymous source that that particular IMSI catcher 'was brought into the country in small pieces and was then assembled by an Israeli company based in Cape Town'.

Verint is a company with its beginnings in Israel and the Israeli surveillance industry. Today, the company has multiple international shareholders and has its headquarters in Melville, New York. It produces IMSI catchers with vast capabilities, as described above. According to the company website, it has branches in more than 180 countries and is the 'global leader in Actionable Intelligence® solutions for customer engagement optimisation, security intelligence, and fraud, risk

[31] IOL, 'Grabber nabbed in big sting', 3 August 2015. See http://www.iol.co.za/news/crime-courts/grabber-nabbed-in-big-sting-1894536

[32] IOL, 'Beware superspy grabber', 27 August 2015. See http://www.iol.co.za/capetimes/beware-superspy-grabber-1906372

and compliance'.[33] In May 2012, Verint announced its appointment of South African representatives to lead its 'SA expansion'.[34]

A former crime intelligence police official with particular knowledge of cyber surveillance (SOURCE F) was also of the opinion that the IMSI catcher seized in Irene was brought into South Africa by Verint. When asked why he thought that Verint in particular had brought the device into the country, the former intelligence official said that it was the company's speciality:

> Look, it's like I just told you. The Israeli's are at the forefront. The Mossad has put a lot into it.

Verint is infamous for the role its equipment played in the mass interception of phone and internet communications for telecommunications company Verizon in the United States. [35] [36] The company's connection to South African intelligence services warrants further investigation.

Samuel Vaknin, reporter in the Middle East and the Balkans with sources linked to Israeli and other intelligence agencies, was of the opinion that South Africa's intelligence forces were most likely utilising an IMSI catcher produced by and Israeli company by the name of Ability.

> Israel doesn't have any other meaningful surveillance equipment except the Ability. There is a single company in Israel that manufactures all of this. Ability is more than enough for South Africa's use. Ability is a very powerful device. It is way, way more than enough for South Africa's needs.

Furthermore, he said that South Africa has a history of purchasing surveillance equipment from Israel.

> The Israelis have been the main suppliers of surveillance equipment to South Africa since the late 70s. During the apartheid regime and later. And since the late seventies – at the very least, possibly before – but since the late seventies at the very least, Israel has been an important if not exclusive supplier of surveillance equipment.

As is the case with Verint, the potential use of Ability's products by the South African government also requires further investigation.

---

[33] Verint website, December 2015. See http://www.verint.com/about/

[34] Verint blog, 'Verint announces South African personnel appointments, introduces region reseller', December 2015. See http://blog.verint.com/blog/bid/319140/Verint-Announces-South-African-Personnel-Appointments-Introduces-Region-Reseller

[35] Wired, 'Shady companies with ties to Israel wiretap the US for the NSA', 4 March 2012. See http://www.wired.com/2012/04/shady-companies-nsa/

[36] R. Sanders, 'Israeli spy companies: Verint and Narus', Press for Conversion! Spring 2012. See http://coat.ncf.ca/P4C/66/spy.pdf

2.3 Capacity for Targeted Interception: Service Providers, Handover Interfaces and the Office of Interception Centres (OIC)

This section deals with the role that service providers play with regard to the interception of telecommunications and their relationships with the Office of Interception Centres (OIC). It gives an overview of the surveillance infrastructure and accounts of alleged misuse.

The Office of Interception centres

The OIC in located at 25 Tambach Road in Sunninghill, Sandton. Members of the police crime intelligence division, the SSA and military intelligence are stationed there, according to a former crime intelligence police official with particular knowledge of cyber surveillance (SOURCE F). The OIC houses equipment that enables intelligence services to monitor the telecommunications of individuals suspected of criminal or terrorist activity. These telecommunications include landline calls, faxes, cellular calls, SMS and MMS messages, internet activity, social network usage, emails and messenger services such as WhatsApp and Skype calls. In short, it includes all voice and data communications on mobile and fixed-line networks.

The centre can also monitor what is known as call-related information or metadata: the time and duration calls, the numbers involved and the location of callers.

The OIC may only intercept information if the designated judge tasked with implementing the Regulation of Interception of Communications and Provision of Communication-related Information Act (Rica) issues an interception direction. By law, no one is allowed to intercept any cell phone, smart phone, fax or telephone communications, or bug a room without permission from the designated Rica judge.

The same holds for obtaining metadata or call-related data – this includes details like the time of a call, the duration of a call and the approximate location of the mobile device at the time of the call – although call-related data can also be obtained with a subpoena from a magistrate. Metadata is stored by service providers for billing purposes and they make this available to law enforcement agencies in hard copy upon instruction from the court. To obtain these records, officials must apply to a high court judge, a regional court magistrate or a magistrate for a court order. This is regulated by Section 205 of the Criminal Procedures Act 51 of 1977.

Law enforcement officials must prove that the intrusion into a person's privacy is absolutely necessary to meet the ends of justice before an interception direction can be issued in terms of Rica. This is also true for a subpoena on call records in the case of a Section 205 application to the court. Significantly, a case docket must be opened before interception can legally take place. To open such a docket, police must gather enough evidence through police detective work in the old fashioned way – without the aid of electronic interception. Thus, if intelligence is gathered via interception prior to the opening of a docket, it is illegal.

The legitimate use of handover interfaces in interception

All telecommunications service providers in South Africa are legally obliged to assist law enforcement agencies in investigations by allowing them access to private subscriber telecommunications upon a judge's or magistrate's order. For this purpose, service providers must, at their own expense, install on their networks what is known as a handover interface. A handover interface can cost a service provider over R100 million, according to an expert in mobile security with inside knowledge of security processes of mobile service providers (SOURCE J). These interfaces are essentially gateways between the service providers' infrastructure and the OIC.

The handover interface duplicates the signal of the user's communications, whether a voice call or any form of data communications (such as emails, Whatsapp messages, social media activity or web browsing activity). Any device connected to the network can be monitored; be it a landline, fax machine, laptop, mobile phone or smartphone. The handover interface is connected to the OIC via fibre optic cables. Rica demands that this interception must not in any way interfere with the communications of the person targeted for surveillance and that it must occur without the knowledge of that person and must not cause any interference with the network's normal operations. While this is a necessity for successfully monitoring suspects who are thought to be involved in crimes, Rica also forbids the disclosure of an interception direction to the targeted person or anyone else. Thus, a subscriber can never know if they were a target for interception.

In order to further explore the relationship between mobile service providers and the OIC, and with a view to establishing the extent of illegal interception, interviews were conducted with several sources, most of whom wished to remain anonymous.

Legitimate targeted interception and the role of mobile service providers

In order to investigate the manner in which major service providers aim to ensure subscribers' telecommunications privacy where lawful interception is concerned, the four major service providers in South Africa (Vodacom, MTN, Cell C and Telkom) were contacted. However, the only meaningful response was received from Vodacom. An interview was held with the company's chief risk officer, Johan van Graan. Van Graan and a designated staff of 14 work closely with law enforcement agencies and the OIC in their investigations.

Van Graan stated that the service provider has strict control over the numbers that are intercepted through the handover interface. He said that the OIC does not possess the capability to access subscriber communications without the assistance of the service provider. Van Graan stated that, with the technology used in South Africa, personnel in the OIC cannot access the handover interface remotely and that only the service provider is able to programme the interface to deliver communications to the OIC. In addition, only four dedicated service provider staff members, who have to receive clearance from the SSA, can programme the handover interface and physically access it.

According to South Africa's Department of Justice and Constitutional Development, the service provider *must* route the intercepted communications to the interception centre, where law enforcement agencies can access it. In addition, law enforcement agencies have to follow strict procedures to ensure their Rica applications are legitimate. For example, only some high-ranking officers in the law enforcement agencies can apply for interception directions.

Furthermore, according to Van Graan, it is practically impossible to hack into the handover interface. This statement was corroborated by SOURCE H, a cyber crime investigator with links to intelligence services:

> It [the handover interface] utilises ghost IP addresses and cannot just be penetrated. The actual hardware is strictly controlled by authorised senior personnel who are vetted.

According to an employee at a mobile service provider (SOURCE K), handover interfaces are highly secure. They are usually stored on the premises of the service providers in highly secure facilities and equipped with alarm systems and camera surveillance. Biometric recognition software is also used as a security measure. A limited number of personnel employed by the service provider (fewer than five persons) have access to and the ability to programme the handover interface. These persons must all be vetted by the SSA. No other person, including employees of the service provider not vetted by the SSA, may enter the facility where the handover interface is kept, unless accompanied by a person with clearance from the SSA.

Both SOURCE K and SOURCE H stated that mass interception (continuous monitoring of millions of subscribers' communication) via service provider handover interfaces was impossible, because the technology did not allow for it. SOURCE K stated that service providers did not record or store intercepted communications, but only sent a duplicate signal of the communications belonging to a subscriber targeted for surveillance to the OIC. Only the OIC record and store the intercepted communications. According to SOURCE J (an expert in mobile security with inside knowledge of security processes at a major mobile service provider), a maximum of 500 subscribers' communications could be intercepted simultaneously at major service providers like MTN, Vodacom, Cell C and Telkom. According to SOURCE H, this number could be as high as 2 500. In addition, SOURCE J stated that the interface had to be specifically programmed for each individual number under surveillance.

In addition, according to SOURCE J, service providers never record or store communications content. SOURCE K said that mobile companies do not store SMS messages and voice conversations as a rule, because there is no practical or financial reason for storing such communications. Metadata is, however, stored, in the form of call data records, since this is used for billing purposes. Call data records also provide information such as the call quality and which base stations were involved in the call, as well as other aspects needed to analyse and optimise the network.

A former crime intelligence official with experience in processing intercepted communications within police crime intelligence (SOURCE G) confirmed this:

> With tower data, you can ask data on a tower for a specific period of time and a specific area, and you can go back in time. You would be lucky if you could still get an SMS. You can get information on incoming and outgoing time of an SMS or calls, but actual SMSes have an expiry date.

Furthermore, SOURCE G described strict processes followed by police crime intelligence services when communications metadata was intercepted. The source stated that, after the necessary metadata is gathered and processed by crime intelligence analysts, the South African Police Services (Saps) were under obligation to return to a magistrate's court for further permissions in terms of section 205 of the Criminal Procedures Act:

> The analysts determine if the communications can be utilised in court. They then guide the police detective in the investigation. That detective repeats the entire investigation, including reapplying to the court for legal permission to intercept the suspect's metadata. He repeats the whole process and builds up a docket, and only then can he go to court.

SOURCE G said that, in terms of intercepting communication content – such as voice calls – procedures are equally strict:

> You are completely encroaching on that person's privacy, so a judge must grant permission – specifically for each number when you are listening to the person's private communications.

Abuse of handover interfaces and service provider provision of metadata

Other sources say that illegal interception through the abuse of service provider handover interfaces is easy and occurs regularly.

According to one counter-surveillance expert who consults for government on counter-intelligence and security matters (SOURCE I), service providers are powerless when it comes to communication monitoring done by the OIC:

> Your service provider won't know if you are being tapped, or intercepted. And they just literally (like you see on TV), once they've got the information on you, on their computers they just tap in, ok it's 083 123 5678, and bang! They're on your phone. They can hear the calls, record the calls, they can see your WhatsApps, they can see your Skype messages. If they want to monitor an individual phone – they don't have to ask the service provider's permission to do it. They don't have to get anything from the service provider. They just connect. There has been evidence that it has been misused, and there have been prosecutions. But then there used to be in the old days before cell phones and before digital signals. It's always gone on. It's just another corrupt practice.

One former crime intelligence official (SOURCE E) told of personal experience of being victimised by former colleagues in the OIC who had an axe to grind with him. The source said that they illegally gained access to his bank statements and cell phone conversations. The source added that one would have to go to great lengths to make sure that your communications were not recorded, should you become a target for surveillance:

> They basically 'hack' into the cell phone number without anyone knowing. Only when the service provider has a court order – that is when they will know about it. But if they do these 'skelm' [underhanded] things they never let the service provider know. And they can listen to it in real-time, and if they do it is automatically recorded. Cell phones are out. The internet is a no-go. Your own house

> or office landline is a no-go. Anything official is out of the question. You have to make an appointment in person with whoever you want to talk to and both of you need to use a telephone booth.

Another former crime intelligence officer [SOURCE F] said the laws protecting personal communication privacy may give the public a false sense of security, and that there is no guarantee that illegal monitoring will not occur at the OIC.

> All the intelligence branches sit there and they monitor as they please. Legally they are supposed to get an interception order. But they have ways to intercept your internet communications. They will not say openly that they can intercept as they please.

The source put this practice down to sloppy detective work.

> The guy that intercepts communications illegally – he hasn't done his job because he is still fishing to see if the person is really involved. He hasn't done a proper investigation. So he will intercept illegally.

There have also been court cases in which illegal interception has been documented.

Notably, in the 2011 case of the convicted drug trafficker, Glenn Agliotti, part of the reason why the case against Agliotti was lost, was due to the fact that cell phone records were obtained illegally during the investigation. In the final judgement, Justice J. Kgomo said the following about the investigations of Saps with regards to disregarding the requirements of Section 205 of the Criminal Procedures Act: [37] [38]

> They could not exclude the manipulation of cell phone records by unscrupulous persons. Further, contrary to their assurances that cell phone records were only issued out upon receipt of a court issued section 205 subpoena, cross-examination of Hilda du Plessis, for example, elicited evidence to the effect that there were instances where she issued out such records well before a section 205 subpoena was even applied for: She relied on the bona fides of a police officer in a faxed message, that she send out to the latter the cell phone records and the requisite section 205 subpoena would follow later.
>
> Ms Heynecke for instance testified that she had furnished the police with about 50 lever arch files full of cell phone records in respect of various people. Nobody could shed any light to this Court what could have happened to all that data because only a handful of data was handed in and used in exhibits in this case.
>
> Abuse of the system by the police was demonstrated by Hodes SC during cross-examination of these cell phone 'exerts'. For example, he elicited evidence to the effect that cell phone records of the accused's attorney; himself, Hodes SC, accused's counsel herein, his (Hodes') father's, also an advocate who has nothing to do with this case; other clients of accused's counsel, Hodes SC like one Peter Skeet; phones of private attorneys' firms and private investigator Warren Goldblatt; among many others, were subpoenaed and obtained by the police from the cell phone companies.

In 2011, the Mail & Guardian reported that a common way for law enforcement agencies to access communications content or call records illegally would to take advantage of long-term state surveillance projects that can last decades. For such projects, large groups of persons may be under surveillance in terms of Rica. In this way, a subscriber's number may be added to an existing project

[37] South Gauteng High Court judgement, 'The State vs Norbert Glenn Agliotti', 25 November 2010. See http://www.saflii.org/za/cases/ZAGPJHC/2010/129.pdf

[38] L. de Koker, 'The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks within the New Standards Framework', Washington Journal of Law, Technology and Arts, 1 October 2013. See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2639462

for surveillance without permission from a judge. [39]

This practice once more suggests that the OIC is indeed able to access subscriber communications without the knowledge of the service provider.

In the same article, a former crime intelligence officer, Deon Loots, went on record to give an account of how his communications had been illegally intercepted by police crime intelligence. Loots told the newspaper that after leaving crime intelligence and becoming a private investigator, he maintained ties with former colleagues still working in police crime intelligence and the OIC and could request (from his former colleagues) metadata or communications content of persons he was privately investigating. He also told the newspaper that, following a dispute with a former colleague still employed by police crime intelligence, his cell phone communications were intercepted and bank accounts were accessed in order to sabotage him personally and professionally. He further stated that illegal interception was common practice within the crime intelligence division.

During the course of this investigation, further testimony of the illegal interception of telecommunications by police crime intelligence was obtained. One source, a retired South African Police Service detective (SOURCE L), attested to approaching mobile service providers on a casual basis to obtain call records and that it was unnecessary to bribe service provider employees for caller information.

> You just had to be nice, then you could get anything. Remember, I was a detective. I only had to say I am from the police, and that I am looking for information. I never even gave anyone a chocolate.

The source also recalled a case of tracking a suspect who had stolen a light aircraft from Wonderboom Airport in Pretoria. The source said that police crime intelligence was able to furnish him with the call data records of the suspect. For example, crime intelligence utilised information from base stations to trace the flight pattern the suspect followed with the stolen aircraft. The source said that crime intelligence also furnished him with the metadata of the suspect's girlfriend, which then revealed the cell phone number of the suspect. Once his cell phone number was obtained, his metadata was intercepted and it was possible to narrow down his whereabouts based on the base station to which the records showed his cell phone most frequently connected. All of this occurred, according to the source, without a single subpoena. The suspect was later prosecuted successfully, and the evidence was accepted in court despite the fact that the defense lawyer brought it to the court's attention that the metadata was not obtained legally. According to the source:

> I just stated that I got the information from a contact. The court accepted it as is.

The employee at a mobile service provider (SOURCE K) said that individual law enforcement agents sometimes abused processes to access metadata illegally in order to sell it for personal gain:

> The police officer as an individual officer gets a court order, a section 205, for a hijacking syndicate with nine numbers that are really about the hijacking syndicate, and the tenth number is about somebody that's in a divorce.

[39] *Mail & Guardian*, 'The Secret State: how the government spies on you', 14 October 2011. See http://mg.co.za/article/2011-10-14-secret-state

> Then we give the information to that policeman, he sells [it] for R20 000, and the aggrieved party in the divorce then says, 'Let's settle, otherwise I will request this information through legal channels'.
>
> We have no control over that. And, when we find it out, we hand it over to the police and they investigate it.

Despite the fact that safeguards are in place to prevent subscriber communications from being illegally intercepted by law enforcement agencies, it would appear that reports of illegalities of this nature are rife. Further investigation is required to establish the true extent of abuse.

2.4 Cyber Surveillance

During the interview with Sam Vaknin (the reporter in the Middle East and the Balkans with sources linked to Israeli and other intelligence agencies), he made the observation that South Africa was known in the international arena for its use of cyber surveillance to carry out targeted interception. Vaknin stated that the South African government was far more likely to carry out this sort of surveillance than mass interception, for instance. In particular, he asserted that the NCC had purchased a license for FinFsher – a powerful software suite that allows for law enforcement surveillance of data communications on a personal computer or smartphone. Specifically, the South African government is known to use FinSpy, a particular product within the FinFisher range that allows state intelligence agencies to infect a target's computer or smart phone with spyware that allows the surveiller to monitor, in real-time, all the user's communications. These communications would include emails, Skype calls and social media activity such as Facebook and Twitter, and messenger services such as WhatsApp or Blackberry messenger. The software is capable of intercepting encrypted files on a computer, turning the computer into a microphone to record conversations within range, and utilise a laptop camera to record visual material within its frame. Vaknin said that South African intelligence was likely to target individuals, such as journalists and activists.

FinFisher 'looks' at a target's communications with a widely used technology: packet inspection. Whenever data is sent – for example, in the form of an email – that email is broken into smaller pieces of data called packets. The packets, much like a packet sent from the post office, contain three pieces of crucial information: an address identifying the sender, another identifying the receiver and the actual content of the message. Packet inspection looks at this information. For instance, one way in which firewalls can protect a computer is to inspect an incoming data packet. The firewall will identify the address of the sender of that packet; if it came from an untrustworthy source, the firewall blocks it. FinFisher goes a step further than this: It uses what is known as deep packet inspection (DPI). DPI can look not only at the addresses connected to a data packet, but at the actual content of the packet.

FinSpy uses a culprit known to most internet users: the Trojan horse. The name derives from the ancient Greek myth in which the Greeks hid inside a giant wooden horse which their opponents – the Trojans – were led to believe was a gift from Athena, the Goddess of War. Once the horse was

inside the city of Troy, the elite Greek soldiers inside opened the gates to the city so that the rest of the Greek army could invade.

As in the myth, the Trojan horse masquerades as a harmless document or JPEG that you receive via email. Once you open the document, the Trojan automatically installs itself onto your computer, disguised as just another file.

The South African intelligence services have never publicly admitted that they utilise FinFisher products. However, The Citizen Lab, a Canadian organisation, has located FinFisher servers on the network of Telkom (a parastatal and major fixed-line and mobile service provider) on two separate occasions – first in 2013 and then again in October 2015. There was virtually no media coverage of the second discovery of FinFisher servers on a South African network and Telkom was never confronted on this occasion. However, in the 2013 case, the parastatal said that, without an official criminal docket being opened by the police, it could not investigate the matter in order to establish who the server belonged to.[40] [41] [42]

No other sources interviewed were familiar with the product. However, since Telkom is a parastatal and in light of the fact that it is sold exclusively to government law enforcement, further investigation regarding the possible use of FinFisher by the South African intelligence services is required.

[40] C. Fuchs. 'The implications of deep packet inspection internet surveillance for society', The Privacy and Security Research Paper Series, July 2012. See http://fuchs.uti.at/wp-content/uploads/DPI.pdf

[41] The Citizen Lab, 'For their eyes only: the commercialisation of digital spying', 30 April 2013. See https://citizenlab.org/2013/04/for-their-eyes-only-2/

[42] The Citizen Lab, 'Pay no attention to the server behind the proxy: mapping FinFisher's continuing proliferation', 15 October 2015. See https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

3. CONCLUSION AND RECOMMENDATIONS

The reports of alleged illegal interception by South African law enforcement agencies are not exhaustively dealt with in this report. Although evidence of illegal interception is hard to find, allegations of similar transgressions from sources completely unrelated to each other abound. In addition, South African law leaves much to be desired when it comes to regulating the state's use of surveillance technology. In light of this, further research into the misuse of telecommunications surveillance and increased advocacy for telecommunications privacy is desirable.

Recommendations for further research are as follows:

Although it is clear that the South African government has a good relationship with VASTech, a major role player in the international market for surveillance equipment (particularly in Africa and the Middle East), more research is required regarding the company's relationship with the government, who the company deals with and to what extent the government is utilising VASTech's equipment. It is a fact that bulk interception facilities located at the NCC and operated by the SSA do exist. It is also a fact that the government helped to develop, at least financially, a mass recording technology of massive capability that has triumphed in the highly competitive, rapidly growing surveillance industry over the past decade. There is, therefore, good reason to believe that the South African government is using VASTech's equipment, and the matter requires further research.

The NCC is not, by its nature, transparent in its doings or held accountable to the public. The true nature of the work done there and the potential for illegal interception still needs to be established.

Although IMSI catchers do not appear to pose as big a threat to telecommunications privacy as do mass interception devices, their use is still unregulated and reports of misuse of these devices as well as their illegal sale to private individuals are ample. IMSI catchers are far more advanced today than they were in 2001 when police crime intelligence reportedly purchased such a device. More recent information on the state's actual capacity in terms of IMSI catchers is required.

Despite the fact that safeguards are in place to prevent subscriber communications from being illegally intercepted by law enforcement agencies via handover interfaces and the OIC, reports of illegal interception are rife. Further investigation is required to establish why these systems are so vulnerable to abuse.

No South African sources interviewed were familiar with the FinFisher product range. However, since Telkom is a parastatal, and in light of the fact that it is sold exclusively to government law enforcement, further investigation regarding the possible use of FinFisher by the South African intelligence services is required.

Appendix A. List of sources

a. A person with close connections to the private sector producing mass interception technology locally. In particular, this person has personal contact with the top management in VASTech. (SOURCE A)
b. A person previously involved in diverse aspects of state security who has intimate ties with a technician involved in equipping the government with mass interception capacity (SOURCE B)
c. A former military intelligence operative with inside knowledge of the workings of the National Communications Centre, the primary interception centre of the State Security Agency (SOURCE C)
d. A former senior military intelligence officer with particular knowledge of counter-intelligence (SOURCE D)
e. A former crime intelligence police official and undercover operative (SOURCE E)
f. A former crime intelligence police official with particular knowledge of cyber surveillance (SOURCE F)
g. A former crime intelligence official with experience in processing intercepted communications within the police crime intelligence division (SOURCE G)
h. A cybercrime investigator with links to intelligence services (SOURCE H)
i. A counter-surveillance expert who consults for government on counter-intelligence and security matters (SOURCE I)
j. An expert in mobile security with inside knowledge of security processes of mobile service providers (SOURCE J)
k. An employee at a mobile service provider (SOURCE K)
l. A former detective in the South African Police Service (SOURCE L)
m. Samuel Vaknin, reporter in the Middle East and the Balkans with sources linked to Israeli and other intelligence agencies
n. Yasmin Omar, attorney for Khalid Rashid, a man who was arrested on 31 October 2005, allegedly with the aid of an IMSI catcher, and later found by the Supreme Court of Appeals to have been illegally deported by intelligence services.
o. Johan van Graan, Risk Manager at Vodacom

Appendix B. CSIR response to Mail and Guardian questions

Date: 14 December 2015

Question 1: Would the CSIR care to comment on the allegations or statements (that the CSIR worked or assisted VASTech to develop interception technology).

Answer: The CSIR is not involved in the development of interception technology or any other technology with VASTech SA (Pty) Ltd. The organisation has not contracted or partnered with VASTech and such technology was not developed through a CSIR project.

Question 2: What was the nature of VASTech SA (Pty) Ltd relationship to the CSIR?

Answer: VASTech SA (Pty) Ltd has been a tenant at the CSIR Scientia Campus in Pretoria since the 1st of February, 2005.

Question 3: Did the CSIR at any stage fund VASTech SA (Pty) Ltd?

Answer: No. The CSIR has never funded any project or partnered with VASTech SA (Pty) Ltd in any technology development.

Question 4: How long was VASTech SA (Pty) Ltd offices located on the CSIR campus?

Answer: VASTech SA (Pty) Ltd has been a tenant at the CSIR Scientia Campus in Pretoria since 1 February, 2005.

Question 5: How long was VASTech SA (Pty) Ltd offices located at the Innovation Hub?

Answer: The CSIR cannot comment on this, the Innovation Hub is best suited to answer this question since it is an independent company from the CSIR.

Question : How long was VASTech SA (Pty) Ltd offices located at the Maxum Business Incubator?

Answer: The CSIR cannot comment on this. Maxum Business Incubator is best suited to answer the question.

Question 6: What other forms of support did VASTech SA (Pty) Ltd receive from the CSIR?

Answer: None.

END.

For more information, please contact:

Tendani Tsedu

CSIR media Relations Manager
Tel: 012 841 3417
Cell: 082 945 1980
e-mail: mtsedu@csir.co.za

Appendix C. The Innovation Hub response to Mail & Guardian questions

Media enquiry

Media house: Mail and Guardian

Reporter: Heidi Swart

1) Did The Innovation Hub or the Maxum Business Incubator ever fund VASTech? If so, how much funding did VASTech receive?

Answer: VASTech was incubated at Maxum Business Incubator during the pilot operation at the CSIR, they left incubation in 2006 and they are now operating from the Stellenbosch technology park. VASTech was never funded by Maxum, we do not fund entrepreneurs.

2) What other support did VASTech receive from The Innovation Hub and Maxum Business Incubator?

Answer: As a start-up company, VASTech was offered space to operate and business mentorship.

3) Was the Innovation Hub and the Maxum Business Incubator aware of the nature of VASTech›s products, in other words, that these products could be utilised for mass interception, which in turn can grossly violate people›s privacy?

Answer: The Innovation Hub was aware of the product and services that VASTech was developing while they were incubated. Their activities and clients were legal. As a government agency, it is our policy to support technology start- up companies and promote their growth in the market