CYBERCRIME AND THE DOUBLE-EDGED SWORD OF STATE SURVELLIANCE IN SOUTH AFRICA

Professor Ashwin Desai
University of Johannesburg, Gauteng
ashdesai1@gmail.com

Running headline –Taking liberties: Cybercrime Cyber-surveillance in South Africa

Ashwin Desai
Department of Sociology,
University of Johannesburg
Kingsway Campus
PO Box 524
Auckland Park
+27 727829611
ashdesai1@gmail.com

ABSTRACT

This article uses the recent cyber attack on one of South Africa's largest financial institutions Liberty Holdings as an entry point to illustrate the challenge of cybercrime for the boardrooms of big capital in South Africa. This breach reinforces arguments raised for enhancing the state's capacity to police cybercrime. Against this backdrop, the article reflects on the debate around the policing of cybercrime in South Africa, highlighting arguments that the way in which the state attempts to deal with this growing problem has also created fears of the emergence of a surveillance state with unfettered powers lodged in intelligence agencies. This debate has been sharpened by recent exposés of the corruption seemingly endemic to South African intelligence services, revelations that some of its leading personnel were gerrymandered to settle internal battles within the ruling African National Congress (ANC), and more shocking, the allegation that a key agency tasked with providing IT to the country's entire public service might have been captured by one supplier.

Keywords*:* Cybercrime, surveillance, Liberty holdings, South Africa, hacking.

INTRODUCTION

> "Dear Valued Liberty Customer, Liberty has been subject to an illegal and unauthorised access to its IT infrastructure, which was largely e-mails and attachments. This matter is with the relevant authorities for investigation. To this end we would like to inform you of the following to help you be vigilant in the protection of your data: 1. Liberty will not send you an e-mail or link for you to change any of your passwords. 2. It is always good practice to ensure you select strong passwords and change them on a regular basis. Should you have any further queries or questions please do e-mail us on info@liberty.co.za or call us on 0860456789. Regards Liberty" (email sent to Liberty clients, 22 June 2018).

With these simple words, the giant South African financial service provider, Liberty Holdings revealed to their customers that their security had been a breached. Reports indicated

that R1.68 billion was swept off the company's R34bn market value (Saturday Independent, 15 September 2018). The episode brought home to South Africans the immense reach of cybercrime and its ability to trespass into the inner sanctums of huge corporates with a global footprint. It also indicates how in this juncture of rapid technological advance, corporates seek to transfer responsibility for security onto their customers.

A new bag of tricks

Over the past decade, research into the relationship between new forms of technology and crime have illustrated how "Drones, tracking devices, social engineering, hacking, encrypted communication have in a short space of time been added to the villain's bag of tricks alongside the crowbar, the knuckle-duster and the gold chains" (Glenny, 2017).

In South Africa, these advances in criminal activity hardly ever enter the public domain, which is generally dominated by cash-in-transit heists. These heists are almost an everyday phenomenon. Given that they take place in very public places and often involve bloody shoot-outs, they are ready-made for television and attention-grabbing newspaper headlines. Cybercrime does not involve AK-47 wielding criminals blowing up vans with cash in crowded urban areas. Cybercriminals work in the background and their weapon of choice is the click of a mouse. Its effects are devastating.

Facilitated by the explosion of mobile connectivity and mass communication across the globe, cybercriminals make bank-robbers look positively last century and home burglars the final hurrah of the Luddite gang. As Wall and Williams point out: "Cybercrime is now the typical high-volume property crime in the UK, impacting upon more of the public than traditional acquisitive crimes such as burglary and car theft" (Wall and Williams, 2013: 409). "As early as 2004, losses from online financial fraud in Brazil were estimated to exceed losses through bank robberies" (Kshetri, 2015: 246). In South Africa, a recent report by Price Waterhouse Coopers states that:

> "At 77%, South Africa's rate of reported economic crime remains significantly higher than the global average rate of 49%. However, this year saw an unprecedented growth in the global trend, with a 36% period-on-period increase since 2016. Economic crime in South Africa is now at the highest level over the past decade. Alarmingly, we still found that 6% of executives in South Africa (Africa 5% and Global 7%) simply did not know whether their respective organisations were being affected by economic crime or not. South Africa has again reported the highest percentage of economic crime in the world, with Kenya second and France third. With half of the top ten countries who reported economic crime coming from Africa, the situation at home is more than dire" (2018: 8-9).

Cybercrime is ubiquitous. Companies, governments, banks and even social media have increasingly become the target of data breaches, fraud, malicious communication, cyber pornography and phishing. As security measures are put in place, criminals find more innovative ways to neutralise them.

Access to personal data is also used in the run-up to national elections, as the recent use of personal data by Cambridge Analytica from Facebook has underlined. It affected millions of internet users and was one of the biggest privacy violations in social media history. But, as Davies argues that while a number of rules were transgressed:

> "Privacy law assumes that individuals have the right to know what their data is being used for before they agree that someone may collect and keep it…Cambridge Analytica were being dishonest and secretive. But while they may not have been true to every letter of their Ts and Cs, and may be in breach of the Data Protection Act, no one, surely, will be surprised to discover that data

> collected in one arena is put to work in another. Using data in novel and secretive ways is virtually the governing principle of the digital economy" (Davies, 2018: 20).

The Cambridge Analytica episode however highlights privacy issues and the inadequate control of personal information voluntarily given to a party. If Facebook were headquartered in South Africa, the onward use of personal information would potentially be regulated by Protection of Personal Information Act (POPI) which will come into effect in end 2018.

In most cases, people using apps on their phones are unaware of how much information they are sharing just by clicking on the app itself. In terms of data breaching and the use of information, cyberspace has become a hacker's paradise.

It raises the question in this context of how we define cybercrime. It certainly needs to be wider than mere unauthorised access to a data system (or hacking) if it is to cover actions such as the Cambridge Analytica misuse of data. What about the use of social media to breach election laws or to manipulate stock prices? While the definition of these offences will still be met whether the prohibited act takes place in print or digital form, offences committed in the digital realm have certain unique qualities. The sheer scope of the offence, the possibility of global (and thus multi-jurisdictional) co-ordination or even out-sourcing of the prohibited act, and difficulties in detection posed by anti-forensic technology and, ironically, privacy conventions – all give crimes in cyberspace a unique character.

Anonymity, encryption and a sophisticated network of clients and technologically savvy criminals means that it is increasingly difficult for global law enforcement agencies to keep up. The enforcement of national laws is made perniciously difficult in that cyberspace provides criminals with the opportunity to direct offences *in real time* against their victims but at great distance from them. Cyberspace is the criminal's new frontier and it can simultaneously cross many borders making "possible near-instantaneous encounters and interactions between spatially distant actors, creating possibilities for ever-new forms of association and exchange" and creating the conditions "for the unscrupulous to perpetrate offences while maintaining anonymity through disguise and a formidable challenge to those seeking to track down offenders" (Yar, 2005: 410-411).

Cybercrime can assume various forms and the way hackers can capture information differs widely: identity theft, phishing emails which attempt to lure customers into clicking on attachments which then give the hackers access to account and personal information and ransomware, where files are encrypted and rendered unusable until an affected user pays for their 'release'. The use of data in innovative and clandestine ways is the leitmotif of the digital economy and give rise to terms like "surveillance capitalism", and "platform capitalism" (Davies, 2018: 20). Cybercrimes are constantly mutating:

> "We have, for example, recently witnessed the birth of the malicious 'supervirus' (such as Flame, Zeus, Spy-Eye and Stuxnet), Scareware and the rebirth of hacktivism. Both Stuxnet and Zeus are professionally constructed complex pieces of software. Stuxnet is a suspected state-sponsored virus that attacks industrial computer systems on- and off-line, seeking out its target of top-secret computer systems that control nuclear enrichment plants. Zeus seeks financial information about its host, whilst also connecting the user's computer to a botnet -a network of infected computers -that broadens the cybercriminal's reach. Scareware extorts money from users and is significant in that it is the first major example of an automated crime where the machine defrauds the user and also sends money back to the criminal… Each of these developments represents a step change on the previous position further challenging existing policing structures" (Wall and Williams, 2013: 410).

Further down the line into 2018, we have new forms of software, or malware as it is known, such as Finfisher which can intercept messages, visit webpages and emails, and Finspy, which is deceptive enough to appear as an ordinary document attached to an email, until that attachment is opened and information on your computer can be hacked. The frightening aspect of cybercrime is that it can jump national borders and many developing countries are scrambling to protect themselves, as Kshetri points out: "In most cybercrimes, offenders and victims live in different jurisdiction. Industrialized countries have resources and a high-victimization level forced them to develop anti-cybercrime institutions... many developing countries lack these conditions" (Kshetri, 2010: 148).

The financial sector and particularly large banking institutions have become popular targets and the amounts stolen have reached spectacular proportions. In what has come to be regarded as one of the largest cyber-heists in history, in 2016 the Central Bank of Bangladesh lost US$81-million when the money was transferred online to the Philippines and subsequently vanished through the casino system (Al-Jazeera, 2018). But the threat goes far beyond financial institutions. In 2014, Sony Pictures Entertainment was hit by a hacking attack, when large amounts of "employee and proprietary Sony data" were stolen. The hackers then "threatened to release the information unless Sony executives paid a ransom demand. Sony declined, and the hackers leaked the data online for the whole world to see. They also unleased malicious software into the company's internal networks designed to destroy much of the company's internal computer systems" (Krebs, 2014: xiii).

While certain countries and continents have hitherto been particularly susceptible to cybercrime, for example the United States and Europe, in the last five years, broadband technology has spread rapidly across the African continent, providing a new feeding ground for potential cybercriminals. As the Secretary General of the International Telecommunication Union (ITU), Hamadoun Toure told Africa News: "cybercriminals see Africa as a safe haven to operate illegally with impunity" (as cited in Kshetri, 2010: 165). According to Vernon Fryer, head of cyber defence operations at security specialist company, NEC XON: "Ethiopia is subject to the most numerous government hacks of any African nation. Zimbabwe is driving a rigorous cyber strategy because they've been hit so hard…Nigeria, South Africa, and Central African Republic are currently three of the hottest cyber attack spots in Africa" (ITWeb Africa, 2018). There are glimmers of hope in Africa, with the ITU's Global Cybersecurity Index citing Mauritius, Kenya and Rwanda as highest in terms of organisational attempts to combat cybersecurity (ITU, 2017: 26).

In South Africa, media stories about law-breaking have always been associated with high levels of violent crime; rape, murder, hijackings and robbery. This has led to calls for more visible policing, 'shoot to kill' cops and a phenomenal growth of the private security industry. Richer South Africans have taken to living in gated communities with state of the art surveillance (Murray, 2011). But these defensive responses are akin to King Canute holding back the waves. The hacking economy can jump these fences and inveigle itself into computers no matter how well burglar-guarded is the suburban study. It has arrived in South Africa with a seeming insatiable appetite, as current statistics show.

In 2014, South Africa lost approximately ZAR50 billion due to cyber-incidents, and in 2015, over half a billion online personal records were lost or illegally accessed. According to computer forensics expert, Danny Myburgh, "79% of all online phishing victims lose their money, and South Africa was the twenty-third highest attacked country in terms of hacking and cybercrime" (Kilian, 2017). In addition to threats on individuals and companies, South Africans are also faced with the fact that governments are increasingly using cyberspace for surveillance of which many citizens are blissfully unaware. By 2015, according to Jane Duncan "South Africa was the third largest named user of FinFisher…FinFisher is a weapons-grade instrument spyware suite sold exclusively to governments…FinFisher is particularly useful for

monitoring security-conscious and mobile targets who make extensive use of encryption, as it can be used to take control of a target's computer as soon as it is connected to the internet…" (2018: 129-30).

In a sociological sense, invasions of privacy perpetrated on the public by cyber-criminals differs only in source from invasions of privacy by state-actors. A criminal may harvest data for nefarious ends but so may a governing party with its hands on even bigger digital forensic tools. While scareware may induce a businessperson to part will hush money, government agents may also induce an opposition candidate to withdraw from an election. While a phishing campaign may cost an individual half their bank balance, tampering with an electronic voters' roll may install a kleptocratic government costing a nation half its growth rate. None of this is to suggest that cyber-surveillance by the state can never be for legitimate purposes. Far from it. But just as Africa suffers from underdeveloped digital security to ward off hacking by syndicates, regulation of its own security agencies to ward off irregular use of intelligence is also notoriously underdeveloped. These then are the Scylla and Charybdis of the African cyber seas: poor security to ward off criminal attacks and poor regulation to ward of political abuse.

And 2018 is no brighter with regards to possible data breaches. The attack in June 2018 on Liberty Holdings, where the financial services giant's computer system was breached and emails stolen has revealed the need for South Africans, individuals and organisations, to have a greater level of preparation and protection of their personal data, while also being mindful of the possibilities of increased state surveillance. Increasingly, internet users and particularly people using cell phones and apps are at risk of their information being unlawfully obtained and used. A recent report states that South Africa "has the third highest number of cybercrime victims worldwide, losing about R2.2 billion a year" (The Cape Argus, 2018). With a burgeoning young population which is technologically savvy and using numerous cellphone apps for banking, as well as a marketplace which is constantly seeking to lure customers into purchasing goods and services electronically, privacy of personal data has become compromised. Personal information bestows considerable corporate advantage to those seeking to sell their goods and services; what Srnicek (2017) calls "platform capitalism" where companies such as Google, Facebook, Amazon, Uber interact to share data and are beginning to stretch themselves into the consumer world of the internet: "Connected home device manufacturers and service providers will seek to overcome thin profit margins by gathering more of our personal data -- with or without our agreement -- turning the home into a corporate store front" (McAfee Labs, 2017). This is proving to be a monumental headache in terms of security of information, as shown in the recent case of Liberty holdings in South Africa.

On Thursday 14 June 2018, the corporation was hit with one of the largest data breaches in South African history. The company was left shame-faced as hackers managed to breach their security systems, infiltrate emails and remove potential files threatening the financial security of some high profile clients (Shapshak, 2018). The hackers then demanded payment of millions from the company to avoid the release of 'critical information': the amount has yet to be disclosed. Insurance companies often keep sensitive personal data on clients, including identity, banking and health information. Liberty Group's CEO David Munro said the data that was affected by the breach consisted largely of recent emails from the company's mailing service (Magubane, 2018). Such data breaches are generally where stolen data is held for ransom and then used for financial gain or to cause harm.

He said the company was in the process of investigating the breach, asserting that the findings of such an investigation would be referred to the authorities. But Andrew Chester, managing director of Ukuvuma Cyber Security, said "the fact that information was so easily accessible demonstrates an "alarming" lack of security in place to protect clients" (Smit, 2018).

As far as the ransom is concerned, the investigation is ongoing and an actual amount has yet to be declared. “In an extortion attack of the sort against Liberty, you're paying for a negative, essentially trusting the crooks for ever more. The good news is that Liberty is being up-front about the attack, trying to find out just how much the crooks got hold of in order to make sure an attack of this sort doesn't happen again” (Moyo, 2018).

In the aftermath of the event, the Information Regulator requested an urgent meeting with Liberty regarding the data breach, which could result in massive fines for the company. They Regulator was keen to establish exactly how the breach occurred, its extent, and extra security measures put in place to prevent another attack. Despite the fact that no client had laid a complaint, the passing of POPI at the end 2018 may see retribution for companies that are involved breaches like that of Liberty.

It is worth pausing at this point to note that, if personal information harvested from customers is maliciously used in ways other than stealing their investments at Liberty, the harmful effects of the Liberty data breach would then pass on to individuals. As is so often the case in other sectors after catastrophic events, for instance an oil-spill: while company profits are happily privatised when times are good, when times are bad, the harm is socialised.

Liberty is one of the largest data breaches of its kind in South Africa and has set alarm bells ringing. It also follows in the wake of smaller incidents, raising the question of South Africa as a new hunting ground for hackers. The number of cases have grown in recent years: in 2014, Eskom, the state’s electricity provider’s payroll system was hacked by employees and in June 2016, hackers managed to steal R300 million from Standard Bank through a complicated and coordinated heist using fake cards at ATMs in Japan (van Zyl, 2016). Email impersonation attacks have also increased in South Africa with cybersecurity experts indicating that in 2018 it has increased by 80% compared to the previous year (Saturday Independent, 15 September 2018).

These are just a few of the cases which have led to a concentration on cyber-security and, as with many governments around the world, South Africa has begun to implement stricter measures, as seen by the new Cybercrimes and Cyber-security Bill. As foreshadowed above, however, sharpening the state’s capacity to deal with cyber-crime may indeed be a matter of creating a double-edged sword.

Policing privacy

> “It’s sometimes said that data is the ‘oil’ of the digital economy, the resource that fuels everything else. A more helpful analogy is between oil and privacy, a concealed natural resource that is progressively plundered for private profit, with increasingly harmful consequences for society at large. If this analogy is correct, privacy and data protection laws won’t be enough to fight the tech giants with” (Davies, 2018: 21).

The threat of cybercrime globally is causing many governments and security agencies to begin implementing stringent preventative measures to tackle what is a rapidly moving network of criminals in cyberspace. Meta-data, such as details about cell-phone messages, digital photographs, emails and internet usage is an abundant source of personal information, and the collection and selling of this ‘data about data’ has become hot property, not only for cyber-criminals but also for governments and security agencies. The latter use it to effectively increase their surveillance over citizens, an issue which has been vociferously campaigned against, particularly by the Right2know campaign and the Media, Policy and Democracy Project.

> “It is pointed out that there is a global trend in cybercrime policy of Governments seeking legal and technical ‘backdoors’ into networks and devices to bypass security measures for ‘good’ purposes and all have been resisted and

decried by digital rights advocates and cybersecurity experts" (ODAC, 2018: 33).

With metadata, an analyst is not privy to the content, for example, of a telephone call. They are not listening in to the call. However, in terms of section 30 (2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) a cell-phone operator must archive records of each client's cell-phone use (their call-logs) as well as each SIM card's unique MSISDN number. This information is to be made available to law-enforcement upon application. Applications for records of past cell-phone use are typically made to a judge in chambers without the cell-phone user knowing that their data is being sought. While the purpose of RICA is to trace the identity of criminal suspects to link them to proscribed actions through metadata, the same information can also link a whistle-blower to a journalist. Whereas tapping into telephone communications is popularly represented as occurring in real time where the actual conversation is monitored, a wealth of personal information can be gleaned from months of call logs simply from the fact that certain calls took place at a certain date and time.

As far as emails are concerned, the Internet Protocol (or IP) address assigned to a user by his or her service provider each time they are active on the internet can give some clue as to the identity of the sender of an email. This IP address is recorded in the metadata of every email sent. A sophisticated user may obscure his or her identity to *the recipient* of the email by using proxy servers. However, his or her internet service provider would record the rerouting by means of these proxies, which tells a story on its own. Should someone legitimately need anonymity to communicate information via email, their internet service provider will likely retain traces of this fact for several months thereafter. Once again, access to a user's internet history is often decisive in proving crimes but the other edge to the generation of this metadata is that it strips privacy when it is legitimately needed.

In South Africa, surveillance has historically been linked to the repression of anti-apartheid movements and activists. Given this recent history, attempts to increase the power of state surveillance agencies raises concern among civil society groups. In 2015, the South African government released the draft of a new bill, The Cybercrimes and Cybersecurity Bill. After an outcry from civil society campaigners who challenged a number of sections of the bill, particularly attempts to criminalise whistle-blowers and journalists accessing information, the bill was passed in Parliament in early 2017. The bill seeks to protect against cyber extortion by criminalising "the unlawful securing of access to data, a computer program, a computer data storage medium or a computer system without authority" (2017: 6). But, Right2know campaign and the Open Democracy Advice Centre have stated that in certain respects, the bill does not adhere to South Africa's constitution. "The Cybercrimes and Cybersecurity 2017 Bill threatens digital rights in significant ways, especially the freedom of expression and association and the right to privacy. The Bill also lacks important checks and balances and increases state power over the Internet in concerning ways" (ODAC, 2018: 15).

In addition to the usual protective measures in the field, such as internet fraud, phishing, data breaches etc., the bill also criminalises malicious communication, i.e. messages that cause harm to person or property. The Bill also seeks to ensure that companies such as Liberty Holdings have adequate protective measures, otherwise they are entitled to call in an Information Regulator to assess the data breach. By declaring particular private sector companies as possessing

> "critical information infrastructure, the State Security Minister can issue directives on the classification of data held by that entity, the storing and archiving of that data, physical and technical security standards, and 'any other relevant matter which is necessary or expedient in order to promote cybersecurity'. There's a lot of devil in this detail. Among other things, it could

> mean that information held by the company that connects you to the internet could now become classified as a national security secret. The 'any other matter' provision could mask serious misdeeds that undermine privacy and internet freedom: most notably, the risk that State Security could grant itself backdoor access to private networks or give itself new surveillance and monitoring powers" (Hunter and Tilley, 2017)

The measures are far-reaching and critics of the bill have suggested that the bill is a threat to freedom of expression and access to information. It

> "gives the Ministry of State Security a large role in governance in South Africa. Placing cybersecurity under the domain of the intelligence agencies makes cybersecurity initiatives less transparent and harder for the public to have a say in them" (Hunter, 2017).

Unlike RICA which, subject to some exceptions, prohibits the interception of communications as they occur, the Cybercrimes and Security Bill would prohibit downloading and distributing a document which one was not authorised to access. Such a law obviously addresses a hole in criminal law to better hold hackers to account. But the scope of legitimate action that it proscribes is wider than RICA. For example, RICA prohibits recording a conversation between two other persons and would thus prevent a whistle-blower establishing a fact of public importance in this way. Arguably, the Cybercrimes and Security Bill would prohibit even downloading evidence other than a communication tending to prove an allegation of public importance. A journalist handed a data-stick with the same evidence of public importance, but which evidence the source had irregularly accessed, would also be committing a crime.

The so-called monitoring and regulation implicit in the push for the new Cybercrimes and Security Bill (2017) hands enormous power to intelligence agencies to target certain individuals in the name of security. This has been seen in numerous cases where journalists exposing fraud and corruption have been spied upon and harassed. It also has a more sinister bent, particularly when governments claim that the exchange of such information is necessary for investigating terrorism or threats to national security. For example, in 2015, leaked intelligence documents known as the *Spy Cables* revealed "a secret agreement between Zimbabwe's CIA and South Africa's state security agency to swap information about NGO's and investigate possible subversive media" (Mare, 2015). Witness the words of Minister of State Security, Dipuo Letsatsi Duba's words at a BRICS conference held in Durban in June 2018, where cyber-security was named as one of the most pressing topics. The Minister said that national security is being undermined by certain role-players and that

> "These actors are in mass media, non-governmental and community-based organisations, foreign multinational companies, religious and student organisations, prominent and influential persons running covert intelligent networks to destabilise other countries who don't share similar views to theirs" (Khubeka, 2018).

Also, the fact that the state has access to information utilising such spyware like Finfisher and Finspy under the rubric of state security means that they can claim it is secret, and therefore are under no obligation to say who, why and where they are spying. Heidi Swart indicates that "a source with links to foreign intelligence agencies told me, that South Africa has 'an ongoing licence for FinFisher. And that it paid, in 2014, $350,000 for the licence.' At the time, that was just over R3.5-million. The source adds: 'I can tell you who has the licence: It's the NCC. The core licencee is the NIA (now the State Security Agency-Domestic Branch)'" (Swart, 2018). At the heart of this debate is access to data about individual citizens, as McKinley points out:

> "Together with the coercive and disciplinary power of the state and the economic and social power of capital, we now have the combined political and economic social power that comes from the vast amounts of permanently stored personal data about entire populations. It is this power that is now being used and abused by the South African state for political and factional surveillance" (McKinley, 2016: 4).

These issues have been thoroughly and painstakingly investigated by the Right2Know campaign and many media journalists who have alleged that they are being spied upon by the state, most notably Sam Sole from the amaBhungane Centre for Investigative Journalism. He states that his phone was being tapped by the NIA while he was carrying out a story on corruption against former President Jacob Zuma in 2008. In June 2018, Right2Know released a report revealing a myriad of examples of journalists who state that they have been and continue to be targeted and spied upon by state security agencies. In 2017, amaBhungane submitted a constitutional challenge around this case, specifically with regards to RICA (, which is supposed to protect citizens from usage of their personal data and is in fact unconstitutional as it has not protected the rights of journalists, as in the Sole case. While Right2Know reveals that the SSA did not try "to disguise Sole's identity or occupation from the RICA judge: the SSA's request for a warrant 'made clear and direct mention of Mr Sole being a journalist and for which media house'" the disconcerting aspect for Right2Know was that "the RICA judge at the time, Judge Khumalo, knowingly signed off on the spying of a journalist" (Right2Know, 2018: 6).

The fact that journalists are being monitored in order to reveal their sources to intelligence agencies means that the state is now indeed trying to protect its own interests at the expense of its' citizens. The events surrounding the Gupta-Leaks in 2017 have also thrown up the increasing use of surveillance tactics, as the Right2Know report shows in the case of Peter Bruce and Rob Rose, senior editors for the Business Day and Financial Mail. They had written articles around the influence over government ministers by the Gupta family and their ability to garner tenders from State Owned Enterprises (SOE's) in a phenomenon that has come to be labelled 'state capture'. Both editors had their phones tapped. It was later found that

> "an MTN employee, Primrose Nhlapo had sold Bruce and Rose's phone records to a private investigator named Nico Smith, a former member of the Hawks. Nhlapo was allegedly paid R3,750 for the information. In terms of RICA, passing on someone's call records is a criminal offence" (Right2Know, 2018: 17).

Jane Duncan in her superb book 'Stopping the Spies' reveals how

> "the Zuma administration (or at least corrupt elements in it) had captured the cluster by removing people who were considered to be obstacles to the state capture project from the investigative and prosecutorial arms of the state, and replacing them with more pliant officials. The intention was to ensure that the agents of state capture would not be held to account….available evidence also points to uses that extend beyond the state capture project, to the containment of growing dissent against the ruling hegemonic bloc more broadly" (2018: 222).

The only reason whereby records can be released is in the form of a warrant, but there is a loophole and that is Section 205 of the Criminal Procedures Act, which "allows law enforcement to bypass the RICA judge and go to any magistrate if the intercept is for call records and metadata rather than the content of messages and calls themselves" (Right2Know, 2018: 3). Civil society organisations have put forward requests for this particular loophole to be closed, a matter which is with the Department of Constitutional Justice. It is clear that state security agencies are acting far beyond their mandate in collecting information, their powers

far-reaching and unconstitutional, not only with respect to journalists and whistle-blowers but all citizens. As Sam Sole points out: "It's the structure of many intelligence services that while they claim to be protecting the interests of the country, historically and institutionally they're often there to protect the king, or whatever the semi-democratic substitute may be" (Right2Know, 2018: 7).

Conclusion

The Liberty Life breach brought home to South Africans the coming of cybercrime and the implications for personal privacy and violation thereof. For a long time, South Africans have battled cheque fraud and credit card cloning. But the Liberty episode has forced a broader and urgent re-think into the mechanisms at hand to combat cybercrime. However, this process has been muddied by allegations that moves on the part of government to stem cybercrime is a subterfuge to increase state surveillance and monitoring powers over citizens. In the South African context, these allegations have been given credence by the move to locate cybercrime investigations under the purview of intelligence agents. This has led to civil society organisations like the Right2Know campaign critiquing the Bill and warning of a potential threat to freedom of expression and access to information. Duncan's warnings in this regard, that draw the past into the present, are apposite:

> "There are important and disturbing parallels between the uses of the intelligence services under apartheid and in the post-apartheid democracy so it cannot be argued that the 1994 transition represented a clean break with the intelligence practices of the past, as there are important indicators of continuity. In the case of the ANC, its intelligence capabilities were geared towards strategically mapping out future scenarios, and its tactical and operational intelligence capabilities focused on rooting out apartheid spies. But it also extended its role beyond counter-intelligence against its apartheid foe, to suppressing political dissent within the movement's own ranks. It should surprise no one that the movement has carried these practices into government…what has changed is that the technical capabilities available to the agencies have increased massively, while legal regulations have not kept up with technological advances. In fact, legal reform of intelligence agencies has been deliberately delayed…There are many continuities of practice between apartheid and democracy when it comes to corporate and state collusion in facilitating crimes that benefit small elites, and secrecy enables these continuities…" (2018: 224).

Under the presidency of Jacob Zuma, like that of Thabo Mbeki, there have been serious, persistent and credible allegations that intelligence agencies were used to fight internal ANC battles and they were trespassed with massive corruption. Even more disconcerting is that the intelligence agencies themselves have been fingered in looting the state purse (Pauw, 2017). Then there are more recent revelations linked to the notion of state capture that

> "SITA, the key State and Technology Agency tasked with providing IT to the country's entire public service, admitted on Tuesday [28th August 2018] to the Parliament's Standing Committee on Public Accounts (Scopa) that the agency had been captured by one supplier-Keith Keating's Forensic Data Analysts. And until quite recently, Forensic Data Analysts had been the only entity that had known the whereabouts of the server as well as the codes to the entire kingdom" (Thamm, 2018).

Add to this situation the nefarious attentions of sophisticated cybercriminals and one appreciates the true depth of the exposure of the public: Its privacy, passwords and personal information is, from more than one side, up for grabs.

LIST OF REFERENCES

Al-Jazeera. 2018. Hacked: The Bangladesh bank heist. 24 May. Available at: https://www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.html (accessed on: 26 May 2018).

Davies, W. 2018. Short cuts. *London Review of Books*, 5 April, 40 (7): 20-21.

Department of Justice and Correctional Services. 2017. Cybercrimes and Cybersecurity Bill. *Government Gazette*, 40487. 9 December 2016. Pretoria: Government Printers.

Duncan, J. 2018. What Ramaphosa needs to do to fix state spying: Part 2 – mass and tactical surveillance. *Daily Maverick*, 20 February. Available at: https://www.dailymaverick.co.za/article/2018-02-20-op-ed-what-ramaphosa-needs-to-do-to-fix-state-spying-part-2-mass-and-tactical-surveillance/#.WznipvV9jIU (accessed on: 4 May 2018).

Duncan, J. 2018. *Stopping the Spies: Constructing and resisting the surveillance state in South Africa*. Johannesburg: Wits University Press.

Glenny, M. 2008. *McMafia: Crime without frontiers*. London: The Bodley Head.

Glenny, M. 2017. Organized crime finally embraces cyber theft. *Financial Times*, 7 March. Available at: https://www.ft.com/content/a038cd98-0041-11e7-8d8e-a5e3738f9ae4 (accessed on: 4 April 2017).

Hunter, M. 2017. How the cybercrimes bill threatens our freedom. *Fin24*, 27 July. Available at: https://www.fin24.com/Tech/News/how-the-cybercrimes-bill-threatens-our-freedom-20170727 (accessed on: 22 May 2018).

Hunter, M. and Tilley, A. 2017. Cybercrimes Bill makes cyberspace less secure. *Groundup*, 28 July. Available at: https://www.groundup.org.za/article/cybercrimes-bill-make-cyberspace-less-secure/ (accessed on: 20 September 2017).

International Telecommunications Union (ITU). 2017. Global Cybersecurity Index (GCI). Switzerland: ITU.

ITWeb Africa. 2018. Africa to set up cyber defence centres to combat threats. 27 June 2018. Available at: http://www.itwebafrica.com/security/513-africa/244452-africa-to-set-up-cyber-defense-centres-to-combat-threats (accessed on: 27 June 2018).

Khubeka, A. 2018. Terror, cybercrime hot topics for BRICS. *Independent on Saturday*, 30 June 2018.

Kilian, A. 2017. Cybercrime becoming a major threat in South Africa. *Engineering News*, 19 September. Available at: http://www.engineeringnews.co.za/article/cybercrime-becoming-a-major-threat-in-south-africa-2017-09-19/rep_id:4136 (accessed on: 20 March 2018).

Krebs, B. 2014. *Spam nation: The inside story of organized cybercrime – from global epidemic to your front door*. Illinois: Sourcebooks, inc.

Kshetri, N. 2010. *The global cybercrime industry*. Berlin: Springer-Verlag.

Kshetri, N. 2015. Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, 18(4): 245-249.

Magubane, K. 2018. Data breach under control and under investigation, says Liberty CEO. *Fin24*, 17 June. Available at: https://www.fin24.com/Companies/Financial-Services/data-breach-under-control-and-under-investigation-says-liberty-ceo-20180617 (accessed on: 20 June 2018).

Mare, A. and J. Duncan. 2015. An analysis of the communications surveillance legislature framework in South Africa. Media Policy and Democracy Research Report, November 2015. 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.
McAfee Labs. 2017. *2018 Threats predictions*. Available at: https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/ (accessed 21 June 2018).
McKinley, D. 2016. New terrains of privacy in South Africa: Biometrics/smart identification systems, CCTV/AlPR, drones, mandatory SIM card registration and Fica. A collaborative research project between the Right2Know Campaign and the Media Policy & Democracy Project.
Moyo, A. 2018. Liberty Group CIO brings out top guns to fight extortionists. *ITWeb*, 21 June. Available at: https://www.itweb.co.za/content/PmxVEMKXKpYqQY85 (accessed on: 22 June 2018).
Murray, M. 2011. *City of extremes: The spatial politics of Johannesburg*. Durham: Duke University Press.
Open Democracy Advice Centre (ODAC). 2018. Transparency in action. Cape Town: ODAC.
Pauw, J. 2017. *The President's keepers: Those keeping Zuma in power and out of prison*. Cape Town: Tafelberg Publishers.
Price Waterhouse Coopers. 2018. The dawn of proactivity: Countering threats from inside out. Global Economic Crime and Fraud Survey. 6th South African edition.
Right2Know. 2018. Spooked: Surveillance of journalists in South Africa. Johannesburg: Right2Know.
Shapshak, T. 2018. Liberty hack the 'biggest breach' yet. *Financial Mail*, 21 June. Available at: https://www.businesslive.co.za/fm/fm-fox/2018-06-21-liberty-hack-the-biggest-breach-yet/ (accessed on: 22 June 2018).
Shaw, M. 2018. Known unknowns: The threat of cybercrime in Africa. Institute for Security Studies. Available at: https://issafrica.org/iss-today/known-unknowns-the-threat-of-cybercrime-in-africa (accessed on: 16 March 2018).
Smit, S. 2018. 'Liberty breach should never have happened' – cyber-security expert. *Mail and Guardian*, 19 June. Available at: https://mg.co.za/article/2018-06-18-liberty-breach-should-never-have-happened-cybersecurity-expert (accessed on: 20 June 2018).
Srnicek, N. 2017. *Platform capitalism*. Cambridge: Polity Press.
Swart, H. 2017. Cyberspying: The ghost in your machine. *Daily Maverick*, 21 February. Available at: https://www.dailymaverick.co.za/article/2017-02-21-cyberspying-the-ghost-in-your-machine/#.WzniC_V9jIU (accessed on 5 March 2017).
Thamm, M. 2018. Key state technology was captured – lock, stock and secret codes. *Daily Maverick*, 28 August.
The Cape Argus. 2018. South Africans losing R2.2 billion a year to cyber attacks. *The Cape Argus*, 21 June. Available at: https://www.iol.co.za/capeargus/news/south-africans-losing-r22-billion-a-year-to-cyber-attacks-15601682 (accessed on: 22 June 2018).
Van Niekerk, B. 2017. An analysis of cyber incidents in South Africa. *The African Journal of Information and Communication*, 20: 113-122.
Van Zyl, G. (2016). Standard Bank computer was hacked in R300m ATM fraud hit – report. Fin24, 30 June. Available at: http://www.fin24.com/Tech/Cyber-Security/standard-bank-computer-was-hacked-in-r300m-atm-fraud-hit-report-20160630 (accessed on: 1 May 2018).
Wall, D.S., & Williams, M.L. 2013. Policing cybercrime: networked and social media technologies and the challenges for policing. *Policing and Society: An International Journal of Research and Policy,* 23 (4): 409-412.
Yar, M. 2005. The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology*, 2 (4): 407-427.