The Context and the International Drivers of Surveillance in the Southern African Development Community

Ernesto Nhanale and Rui Verde

May 2023

The Context and the International Drivers of Surveillance in the Southern African Development Community

Ernesto Nhanale
Rui Verde

African Studies Centre, University of Oxford

This report was commissioned by the Media Policy and Democracy Project (MPDP). Supported by a grant from Luminate

The MPDP is a joint project of the University of Johannesburg's Department of Communication and Media and the University of South Africa's Department of Communication Science.

May 2023

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

Abstract

This report is a first attempt to present an overview of the facilitating context and the main private international drivers of digital surveillance in the Southern African Development Community (SADC) region. Based on interviews and various materials produced in each country, the report looks at the factors dictating electronic surveillance in SADC countries and maps hypotheses, and indications about the type of international actors that promote mass surveillance technologies in the SADC, including what problems are common and which are the most frequent actors.

The report identifies several international actors that have been playing a decisive role in the supply and adaptation of the most sophisticated technologies.

The important conclusion is twofold: there would be no effective electronic surveillance in SADC without the assistance of companies form other foreign countries. And, as far as it is perceptible, private companies are increasingly occupying a prominent role in external collaboration regarding the provision and training in electronic surveillance technologies which is clearly dangerous.

Keywords: International drivers of surveillance, SADC, China, Israel, USA, Electronic surveillance private companies.

Table of Contents

Introduction

"The growing accessibility of monitoring products in Africa has been made possible by the sales of foreign technology supported by soft loans, primarily from China. In addition to Huawei and other Chinese firms, which have built roughly 70 percent of the 4G network infrastructure on the continent, private cybersecurity and surveillance firms from Israel, the United Kingdom, Germany, and Italy, among others, have also been active in Africa." (Jillil, 2020, para.3).

This is the starting point of this work. The discovery of leading private foreign suppliers of electronic surveillance technology in SADC countries.

The chosen perspective is not about the export-facilitating activities of surveillance equipment by the international industry- as Privacy International puts it (Privacy International s/d), but the domestic use of such materials, that is, the presence of foreign technologies in SADC countries, since, as we will see ahead, most companies operate in a multinational environment with subsidiaries in various parts of the world, allowing them to easily overcome legislation that hinders exports.

Our previous research demonstrates that electronic surveillance activities in SADC have little respect for the law in force, rather operating outside the law or without considering its existence. Therefore, this work seeks to understand which international companies and from which countries support the expanding electronic surveillance occurring in Southern African Development Community SADC. Starting from an overview on the various surveillance trends and their impact, as presented in the first chapter below, it then analyses several specific countries according to the sources available, as such as credible reports and direct interviews.

The methodological basis of the work are the direct interviews taken with researchers and former security officials having as background the reports that other colleagues from the Media Policy and Democracy Project presented.

This report does not represent a detailed coverage of the topic in the SADC, but a starting point to try to identify the main international actions. It is, therefore, an introduction to a topic that needs further investigation and whose sources are still very difficult to obtain. Could be described as a first layer of research. Also, it focusses on private companies rather than in states, as the latter's activities are generally more secret and opaquer, while companies to some extent must publicize their successes and are therefore more exposed. We found that this happens mainly with Israeli companies that have aggressive marketing, unlike Chinese companies that are more guarded.

Chapter 1: The Background: Political, Legal and Technological Context

Before responding to the question about the major international drivers of electronic surveillance, which is the central question of this analysis, this chapter aims to examine the factors dictating electronic surveillance in SADC countries. What policy and legal environment characteristics of these countries encourage electronic surveillance?

The political and legal environment favourable to surveillance

Most democracy and freedom indexes tend to show that most southern African countries are characterised by severe restrictions on freedoms, and in some cases, by regression to authoritarian systems which have severe control of freedom of expression.

A review of *The Economist's Global Democracy Index* shows that the DRC is an authoritarian regime, ranking 164 out of 167 countries assessed in the ranking released in 2022. Other authoritarian regimes include Zimbabwe (at position 133), Angola (at position 122) and Mozambique (at position 117). Zambia (ranked 80), Tanzania (ranked 93) and Madagascar (ranked 83) are classified as hybrid regimes which, despite having democratic characteristics, retain some elements of authoritarianism. Countries such as South Africa, Botswana, Swaziland, and Namibia are in an intermediate position and are classified as democracies, but are of an imperfect nature, in what the Index calls "Flawed democracies" (The Economist, 2022). These data on the tendency of the SADC countries to authoritarianism are relevant to understand how these political regimes become a fertile ground facilitating an environment of electronic surveillance. It should be noted that SADC countries (Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic Tanzania, Zambia and Zimbabwe) do not exactly correspond to Southern Africa. Nevertheless, the juxtaposition is sufficient.The data like those mentioned above, shows that there is a direct relationship between authoritarian contexts and restrictions on freedom of expression, with the use of technologies to enhance the control and surveillance of citizens.

The existence of laws or part of laws that promote an environment of surveillance and excessive control of freedoms is one of the problems that are prevalent in several SADC countries. While the technological advances sometimes promote a legislative environment that is more consonant to the protection of citizens' data, part of the member states find opportunities to regulate and restrict freedoms. In some countries, surveillance has been carried out under the cover of state security laws that are contrary to the principles of fundamental freedoms and rights defined in the constitutions. Several examples can be mentioned: Zimbabwe has a history of surveillance through laws that seek to promote national security, like the Official Secrets Act and the Interceptions of Communications Act (Ndlela, 2020). In Mozambique, there are instruments that allow digital surveillance of journalists, as well as others that limit the freedoms of the press, such as Law nr. 12/75 of State Secrecy and Law nr. 19/91 of Crime against the State Security (FES & MISA, 2018).

In some cases, data protection and cybersecurity laws are used to keep an eye and repress freedoms of expression and the right to information. Zimbabwe's first drafts of data protection and cybersecurity laws were widely contested by civil society in 2020 for their mismatch with international standards on

the protection of privacy and personal data, even introducing mechanisms for invasion, intrusion, monitoring and recording of personal data. Of the various problems mentioned, the proposed laws created formal mechanisms to collect and control personal data instead of protecting citizens' data, as well as serving to police and persecute political opponents (Ndlela, 2020; MISA Zimbabwe, 2020). As Freedom House (2022) reported, insulting the president is punishable by imprisonment under the 2016 cyber-security law, as is posting "offensive" messages. In Zimbabwe, the amended penal code, Official Secrets Act and the new Cyber Security and Data Protection Act continue to be permissive to surveillance. In Zambia, for instance, the Data Protection Bill, the E-Commerce Bill and the Cybersecurity Bill aim to address "social media lawlessness."

Accordingly, to the MISA Report on Freedom of Expression (2019–2020), if not aligned to international standards and best practice, legislation may inhibit freedom of expression and media freedom. The same report shows that:

> *Namibia does not have adequate oversight mechanisms to enable legitimate, proportionate and necessary communication surveillance in the digital age. The current legislative regime including the Namibia Central Intelligence Services Act of 1997 and the Communications Act of 2009 (especially part 6, section 70–77) raise serious concerns about infringement of privacy and surveillance.*
> (MISA, 2021, pp 20–21)

The implementation of Part 6 of the Communication Act of 2009 in Namibia represents a threat to the National Constitutional protected rights to privacy, along with other associated rights (Links, 2021). Accordingly, to Links, implementing this Act will turn Namibia into "another African Surveillance state as legally questionable state surveillance-enabling regulations are pushed towards implementation under the guise of fighting crime and protecting national security" (2021).

The same example can be given from Lesotho, where the parliament passed a cybercrimes law in May 2022 which prescribes high fines and heavy prison sentences, significantly affecting freedoms of online expression and privacy.

Apart from flawed legislative strategy on data protection and cybersecurity, countries in the SADC region are adopting new practices of introducing articles or provisions in various laws that open space for electronic surveillance or restrictions on online freedoms of expression. More than fighting cybercrime, this legislation has been seen as a mechanism to be introduced to persecute opinion-makers, thereby reducing the space for online criticism, press freedoms and civic and political expression (Moyo, 2022).

The legislative trend proactively initiated by the states of the SADC region with the aim of institutionalizing surveillance and, consequently, facilitating the action of the International Drivers for the sale of their electronic surveillance equipment has been complemented, in the last few years, by an intensification of the adoption of laws permissive to surveillance with the purported aim of prevent money laundering and combat terrorism, stimulated by multilateral agencies to support development. This second aspect is confirmed by the examples of Botswana and Mozambique. There threats of an international nature, such as global terrorism, rather than reasons of internal character of the countries led to the adoption of legislation that in last instance create grave hindrances to the exercise of basic freedoms. In these situations, the countries themselves use the demands of multilateral institutions for the adoption of mechanisms against terrorist practices, money laundering and drug trafficking which promote more restrictive laws, as well as the invasion of citizens' private data. The most recent experience was reported from Botswana, where the government, through the Minister of

Defence, Justice and Security, introduced the Criminal Procedure and Evidence (Controlled Investigations) Bill in 2022 for passage through Parliament, in response to the recommendations of the Financial Action Task Force (FATF). This draft law introduces a role for agencies to intercept personal communications on money laundering and associated offences without a court warrant. On the other hand, the proposed law would also have allowed investigators to assume multiple false identities, with the home affairs directors instructed to assist with relevant documents. Although still unapproved and strongly contested by civil society organisations, this law poses a major risk of formalising mass surveillance in Botswana (Mguni, 2022).

In Mozambique in May 2022, the government sent a draft amendment law to parliament establishing the specific legal regime applicable to the prevention, repression and combating of terrorism and actions related to terrorist acts and organisations, which states in article 19 that "anyone who by any means disseminates information classified under this Law shall be punished by imprisonment from 12 to 16 years." In turn, paragraph 2 of the same article states that the one who intentionally disseminates information, according to which a terrorist act has been or is likely to be committed and knowing that the information is false, is punished with imprisonment of 8 to 12 years. MISA Mozambique's worries (2022) on these articles has to do with the fact that the laws intend to create a space of restrictions on circulating information, and exercising arbitrary control on the freedom of opinions, in a context in which the country is fighting violent Islamic extremism in the province of Cabo Delgado. After a public debate that involved the intervention of local civil society organisations, these provisions have undergone some changes in Parliament, but still represent a warning of a constant environment of control initiative of digital spaces under the argument of "State Secrecy."

It should also be noted that Mozambique and Namibia are among the countries that approved regulations for compulsory registration of SIM cards, thereby removing anonymity from short message communications. The regulation was introduced in Mozambique in 2015 after being tested in the context of demonstrations against the cost of living in 2009 and 2012. Namibia approved the same instrument in 2021 as a mechanism to control and combat crime (Links, 2021).

Collective Surveillance Technology Projects

In recent years, in almost all SADC countries, cases of surveillance have been reported. This occurred mainly to limit civic and political freedoms, and targeting journalists, activists of civic organisations and opposition party politicians, especially in countries with dominant party systems.[1] The surveillance apparatus aims to do more than address the interest of fighting crimes or even monitoring risks of attacks against the security of states. In many situations, it aims to control spaces for exercising opinion and press freedoms, perpetuating the practices of authoritarian governance, and intimidating and reducing the spaces for denunciations of bad governance. Therefore, in many cases, rather than using surveillance technologies to fight crime and threats, state security agencies are used to limit the spaces for citizenship and digital democracy.

In South Africa, journalists and leaders of civil society organisations were recently victims of constant digital surveillance. In an article published in the Mail and Gardian, Sikhakhane illustrates the impact that digital surveillance has on activists from civic organisations, civic movements or

1 Countries such as Mozambique, Angola and Zimbabwe are examples of dominant party systems in which, even after elections, the same parties (linked to the independence movements) remained in power, often limiting the space for the opposition to act.

even organised groups claiming their rights in the following account:

> *Several members of the organisation have been assassinated while others spent months in jail on bogus charges. Some of them have had to go underground and cut off communication with their families for fear that their phones will be monitored and they will be physically followed around. Now with the rise of digital tools at the hands of corporations and the government, the threat to activists is even larger.*[2]

In the various reports on surveillance that were analysed, as well as the reports produced by the Media Policy and Democracy Project (MPDP) journalists, security agencies, defence, and security forces, including the police, have been the State entities motioned repress demonstrations, journalists, and political opponents. In many places, corruption and misgovernance are rampant, activists and bloggers are subject to surveillance and, in some cases, are even arrested and face prison sentences.

The use of public high-definition surveillance cameras, the obligation to register SIM cards, phone tapping with almost no specific regulation or clear public information on the destination of the data collected are novel ways of digital surveillance. In almost every country, especially Mozambique, Zimbabwe, Angola and South Africa, there are reported projects for installing public surveillance equipment, in projects known as "Smart Cities." In Johannesburg, South Africa, in a public-private partnership with the company, Vumacam, the city is expected to install more than 100,000 cameras in the streets in addition to the 5,000 already installed and 216 of which are in partnership with IBM (SAIIA, 2021).[3]

All of this equipment has a sophisticated capacity to collect data and send it to central controls in real time, as well as to use artificial intelligence to recognise movements considered "suspicious." However, in many cities, such as Maputo and Johannesburg, violent crimes have even been occurring in spaces where cameras are installed, but many of the crimes remain unsolved. There is, however, evidence that this equipment has been used to repress public demonstrations. From a human rights perspective in South Africa, "Vumacam's smart camera network has already generated controversy around issues of racism and civil liberties" (SAIIA, 2021). The Zimbabwean government has an identified plan for developing "star cities" through a plan to be developed between 2020 and 2030. The project involves establishing a national data centre that will converge data from various sectors of activity, which will include individual citizen data, as well as interconnection with the public safety camera system installed in some cities, such as Harare. Besides following a Chinese model, since Huawei Technologies was a consultant on the project, one of the great fears of the project's negative impacts has to do with weaknesses in data protection laws that could open space for abusing citizens' data and allowing their access without the courts' authorisation (Ndlela, 2020).

2 https://mg.co.za/opinion/2022-06-19-state-is-putting-us-at-peril-say-activists/, accessed 23 June 2022

3 https://saiia.org.za/research/the-city-surveillance-state-inside-johannesburgs-safe-city-initiative/

Chapter 2: The Most Influential State and Private International Drivers of Surveillance in SADC

One cannot imagine that surveillance in SADC countries continues to be something of a "cloak and dagger" activity. As a result of allegations by Edward Snowden and others, we know that in the global north most surveillance is carried out by sophisticated electronic means (Snowden, 2019). Snowden's revelations showed us how the Information Communications Technology (ICT) apparatus—using hardware and software services as well as infrastructure—were designed and/or used by U.S. government agencies and corporations as a framework for domestic social control and projection of power against state actors as well as masses of foreign citizens. Snowden revealed that the US international surveillance system, in cooperation with other members of the Five Eyes (Australian, United Kingdom, New Zealand, and Canadian intelligence agencies), operated at all different layers of telecommunications: from the physical layer, with the fibre optic cable clamp submarines collaborating with "interceptor partners" like commercial cable operators (British companies BT, Vodafone Cable, and American Verizon Business) and by cooperating with operators of telecommunications, such as AT&T, to attaching surveillance equipment to routers and company switches and redirecting the information traversing them to the NSA (Snowden, 2019).

A kind of similar pattern, though perhaps not as sophisticated, is discernible in southern Africa. Albeit countries such as Zimbabwe have already admitted that they cannot directly afford or do not have the internal capacity for the kinds of IP based SIGINT surveillance that Snowden revealed, they embarked in fruitful partnerships, mostly with Chinese corporations. As Privacy International states "Low-income countries are providing a ready market for Chinese developed technologies and the Chinese backed loans needed to finance the acquisition of these potentially restrictive technologies." (Privacy International, 2021, para.20). Nevertheless, others as Angola apparently have a good electronic surveillance apparatus using expensive and advanced means, that although are bought outside are adapted for the local needs by national engineers (Anonymous retired intelligence officer, 2022[4]). The same officer describes well the Angolan system saying that the Angolan security system was inspired by the Soviet KGB. In the 1980s, several agents of this organization were in Luanda setting up the various human and electronic surveillance systems. This implied that, at the start, the machinery was also essentially Russian, but within the time it evolved towards a multinational technological endeavour. Also, initially, much of the service's operation was based on brute force and fear, but the need to respond to sophisticated external threats such as those from South Africa and the CIA forced the Angolan services to develop counterintelligence techniques more comprehensively. To this end, they began to hire "external consultants" from an early age, usually with links to the Soviet Union, but also to European Union countries with oil interests in Angola and Israel. There is thus a widening of suppliers of experience and espionage material. This mix became the cornerstone of Angolan intelligence. To maintain the country's independence and sovereignty, they are not dependent on anyone and buy from everyone, states and private companies. Thus, the sovietization of services was abandoned and Israelis, Americans, and French were seen in Angola supplying material.

4 Private interview, September 2022.

This trend continues today and has been extended to China. In terms of telecommunications and CCTV surveillance, China through its private companies has become Angola's main supplier and trainer. (Anonymous retired intelligence officer, 2022).

The interviews we carried out confirmed by the MPDP research has shown a continued and persistent trend towards expanding electronic surveillance in southern Africa, not just in Angola or Zimbabwe, but throughout the region. This also became very clear in the research reports developed in the project and already published (MPDP, n/d). Naturally, advanced technology used everywhere cannot just be based on local technology that simply does not exist. In fact, behind all the surveillance machines developed in the SADC states, whether in Angola, Zambia or Namibia, there are international actors who provide technology, training and operations (Abdulrauf, 2018).

Curiously, in the literature review carried out and in the most modern reports from the MPDP project about international digital surveillance in Southern Africa show that the US's role was not the most conspicuous country. Strangely, Russia's role is similar. Perhaps President Trump's categorisation of "s…holes countries" (Walters, 2018) still echoed in the US's operations of ICT in Africa or they are so much more refined nowadays that they are practically undetectable. Nevertheless, recently, Tony Roberts—a research fellow at IDS—referring to Sub-Saharan Africa emphasised that,

> *Social media is used, for example, to profile citizens and commodify this data for use in covert election manipulation by political public relations firms, while signal interception of internet or mobile data is facilitated predominantly by US and Chinese companies selling AI-based systems that enable remote, automated keyword searches of private communications,*

adding that "these companies include the likes of IBM, Palantir, and Cisco in the US" (Skelton, 2021, 20-21 para.). Russia appears to prefer sending Wagner teams overusing electronic equipment (Fasanotti, 2022). In fact, the Wagner group, considered as a kind of Putin´s tool for Africa, intervening in several African countries, from the Central African Republic to Mali, passing through Mozambique fiasco. But they represent Russia's bet on brute force rather than sophisticated intelligence. (ACLED, 2022). This does not imply that there is no direct Russian collaboration with various African intelligence services. Specifically with Angola, for historical reasons, this collaboration remains very intense, however, it seems to be in the area of information exchange and access to databases (Anonymous Intelligence Services Angola, 2022)

Regarding the US is to be directly referred at least in Botswana, where there are several mentions to an Access Data and a Forensic ToolKit (FTK) that the police force used to extract information from electronic devices, including those that were locked (Balula, 2021). The FTK is a computer forensics software made by the Access Data corporation and scans a hard drive looking for various information. This company is owned by Exterro Inc., a company based in Oregon, US, and an expert in legal governance, risk and compliance (GRC) solutions that enable one to address privacy, compliance, investigation and litigation risks more effectively and at lower costs (Exterro, 2022). It receives investments from Leeds Equity Partners, "a family of funds that invest exclusively in the Knowledge Industries. Founded in 1993, Leeds Equity Advisors has managed over $3.5 billion of capital across a broad spectrum of companies within the Knowledge Industries" (Leeds Equity Partners, 2021). This is a New York, NY, United States based entity.

Beyond USA, several reports point to large foreign involvement in electronic surveillance activities. For instance, in Angola, a detailed and

in-depth Israeli intervention was described and analysed (Verde, 2021). It held that

> *Israel became a place of training for future Angolan intelligence agents–and through the hiring by Angola of retired Israeli intelligence officers, the purchase of sophisticated surveillance materials and the intervention of businessmen and private companies for the purpose of intelligence collection began [and a deep intervention of Israel in Angola occurs]. Over the past few years, there has been a deepening of Israeli collaboration with Angola's intelligence services and elites.*
> (Verde, 2021, p. 5).

It is inconceivable to think about Angola's intelligence collection occurring without Israel.

Somewhat surprisingly, Israel is one of the main actors in electronic surveillance in SADC, with its interventions occurring in several countries, not just Angola. In Botswana, Tachilisa Badala Balula (2021) informed that the Directorate of Intelligence and Security (DIS) was a regular consumer of Israeli products and services. Balula wrote that "DIS had engaged an Israeli company to supply it with a spyware that has the capability to spy on emails, Facebook, and Twitter" (2021, p. 5), and reveals that the DIS would be one of the several world intelligence agencies using Circle Spyware from Israeli hackers. This software exploits weaknesses in the global market's mobile phone systems in order to snoop on calls, texts and phone locations around the world (Balula, 2021). The same researcher adds that "media has also reported that the Botswana Police Service has acquired a Universal Forensic Extraction Device (UFED), sold by an Israel-based company, Cellebrite" (Balula, 2021, p. 5), emphasising that such technologies are apparently able to extract information from phones and computers, break into locked devices and decrypt information. It could be said that Israel's technology created an "open field" for an expanded role of Botswana's intelligence services. Therefore, Israel pontificates in Botswana being a great and, possibly, the main, international actor of surveillance in the country.

It is well known that Botswana is generally represented as a role model for Africa in economic and institutional terms (Robinson, 2013). Robinson argues that a successful Botswana is the result of its institutions, which promoted a more stable and accountable government than elsewhere in Africa (2013). As a result, there is great trust in its institutions. A problem arises when it is verified that technologies that Israel made available can be used in degrading this institutional trust. The core of Botswana's success may then be at stake.

The Israeli companies operating in Botswana are allegedly privately owned and are not a state venture. Specifically, it was possible to identify the so-called Circles, which were acquired in 2014 by an affiliated of the to the now infamous NSO group. And Cellebrite DI, this is an Israeli company that manufactures data extraction, transfer and analysis devices for cell phones and mobile devices. It provides the industry's most advanced technology and services trusted by law enforcement officials and businesses across the world (Cellebrite, n/d). Although Cellebrite presents itself with a veneer of strict legality and assisting law enforcement agencies according to the rule of law, Sam Biddle and Fahad Deshmukh wrote that Cellebrite devices were responsible for the jailing and torture of political activist, Mohammed al-Singace, in Bahrain (2016). They argue that authorities from Bahrain had access to Cellebrite's technology and were willing to use it as blackmail against political dissidents. In this case, they admit that the data vacuumed off Singace's Samsung phone was used against him in court, and also provided a basis for suspicion, evidence of criminality and pretext for torture.

Curiously, although being registered in Israel, the company was acquired by Japanese Sun group. This means that although branded as Israeli, Cellebrite is owned by Japan and at the same time it has several subsidiaries, CelleBrite USA

Corp., BlackBag Technologies Inc., Cellebrite Asia Pacific Pte Ltd, based respectively in the USA and Singapore. Therefore, in the end it will be difficult to describe Cellebrite as an Israeli company or to try to follow the legislation that allowed it to export to Botswana, as they could make their shipments from different countries, namely, Israel, Japan, Singapore, and USA.

The NSO corporation is more famous than Cellebrite and not for good reasons. It is also an Israeli company founded in 2010, and is the owner of the successful Pegasus system, the spyware that can be covertly installed on mobile phones (and other devices) which run most versions of iOS and Android. NSO is also difficult to define in terms of country relevance. Although initially based in Israel, evidence was published mentioning links with Cyprus and Bulgaria. It is referred that the corporation developed his operations by the export control regimes of Israel, Cyprus and Bulgaria (Pegg and Lewis, 2021).

The existence of these companies and devices in Botswana (and other countries) confirms Gadi Perl's (2022) analysis, stating that

> *the built-in secrecy in intelligence matters. No sunlight illuminates their operations. Material is either censored by the agent themselves, or some of it is deemed classified, so that it doesn't appear in an investigation file, and what remains is often papered over so that the original source of the information remains concealed.*

The same interference from private international companies was detected in the DRC. In an interview given to us, Jean-Jacques Wondo[5], a military expert from DRC assures that in his country there is indeed a proliferation of private security companies due to the inefficiency of the army, police and public security services. It is particularly in the mining provinces of Katanga and Kivu and in Kinshasa that we see the development of these companies. MER Group, a form of Israeli private security collaborated with the Kabila regime in Congo. And firms like G4S Security also have subcontractors in Congo. (Wondo, 2022).

Also, Trésor Maheshe's and Musole Jean-Paul Mushagalusa Rwabashi's (2021) research about digital surveillance in the DRC made several Israeli companies' involvements clear. They reported that the "government of former President Kabila had equipped itself with various technological means, which allowed it to wiretap opponents and activists, especially during electoral periods characterised by a dizzying increase of human rights," adding that various international media outlets reported the "involvement of Black Cube, a private Israeli intelligence company in carrying out this targeted surveillance since 2015" (Musole and Rwabashi, 2021, p. 5). Therefore, there is another Israeli company involved: Black Cube. This is the same company that acted on behalf of former billionaire, Isabel dos Santos, against the government of João Lourenço within the scope of the so-called "fight against corruption" campaign that the President of Angola promoted (Cotterill & Croft, 2021). Black Cube promotes itself as being created by a "select group of veterans from the Israeli elite intelligence units that specialises in tailored solutions to complex business and litigation challenges" (Black Cube, 2010). Black Cube has headquarters in Tel-Aviv, London and Madrid, therefore again, Israel is more a brand than an indication of regulatory law.

There is a pattern in this kind of " Israeli" intervention. It does not appear to be state or para-state action; that is, it is not in direct defence of the State of Israel's interests. It appears that people of Israeli nationality who call themselves former Mossad agents and possess advanced surveillance technology have formed private companies that sell their products all over Africa, and that companies are not necessarily Israelite. They do sell these products to governments or opposition groups, irrespective of the greater or less democratic government.

5 Email interview, Sept 2022

As we discovered in a previous report, these activities do not promote the rule of law or state-building in Africa, and typically have disruptive characteristics (Verde, 2021).

An Israeli human rights activist[6] that we interviewed emphasized that Israel civil society is opposed to any involvement of employees of NSO or similar companies, or Israeli government officials, assisting various African rulers in the monitoring and oppression of human rights activists, journalist, opposition figures and civil society elements. (Interview Israeli Human Rights activist, 2022). Curiously, he was assertive referring that when those Israeli citizens call themselves former members of the defence forces or the Mossad, this is usually an indication of cynicism and bad faith. Such people are not interested in using surveillance software for monitoring truly harmful elements. Mentioning NSO, the same activist considered that NSO as a brand is probably finished. However, these technologies are out there, regardless of whether NSO uses them. Cynical players (for example, the Israeli or Saudi governments) are likely to use/ continue using these in the future, as they are not likely to be held accountable. (Israeli Human Rights activist, 2022)

However, it is not just Israel that is referenced in the research we carried out, despite its prominence that must be underlined.

In Namibia, Admire Mare (2021) tells us of the strong influence and intervention that China has on digital surveillance. He presents the hypothesis, but does not definitively conclude, that Huawei's lucrative contracts with all of the major telecommunication operators can imply that they have access to Namibia's national key point infrastructure, making it possible that Huawei can cooperate with certain political elements to install surveillance technologies on the network infrastructure (Mare, 2021).

Referring to Angola, Domingos da Cruz,[7] an Angolan academic and known activist, asserts that, beyond Israel's assistance, several reports highlight the role of China as perhaps the most relevant contributor to helping the country create centres of monitoring by cameras throughout the land, having built two that are already in operation. He also adds that

> *the Chinese government, through ZTE and Huawei, provide technology and support to all defence and security sub- sectors in Angola. In addition, they have provided specific technologies for telephone and internet spying. This additional support from China targets well- identified groups, such as activists and opinion-makers, and penetrates the internal communication systems of civil society organisations.*[8]

Huawei, which also has large contracts in Zimbabwe and Mozambique, is one of the most discussed companies in Africa and around the world. The US government implies that Huawei has certain obscure links with the Chinese Security system and is a danger to the security of communications in other countries. The US's distrust of Huawei began during President Donald Trump's term in office, causing many to think it was merely another whim of the unstable American President. However, under the present Biden administration, in March 2021, the United States Federal Communications Commission (FCC) designated five Chinese technology firms as being an "unacceptable risk" to American national security, in which Huawei stands out. At the same time, President Joe Biden's government has imposed new restrictions on some Huawei suppliers on the export of items intended for use on 5G networks. Washington assumes that Beijing can use Huawei equipment to spy on US residents.

6 Email interview, July 2022

7 Email interview, August 2022

8 Idem

About China, Domingos da Cruz, an Angolan researcher and activist mentions that in his view the Angolan regime is among the beneficiaries, be it of technology or human resources. He says that the is in this framework Angola-Chinese framework provides for an authoritarian Angola-China partnership which built, equipped, trained the technicians/agents, and inaugurated in 2019, in Luanda, the Integrated Public Security Centre (CISP). By the time of their inauguration, more than 700 cameras had been installed around Luanda. These cameras are capable of facial recognition, a function that enables surveillance beyond cyberspace, such as suppressing protests on the ground. Besides the cameras, the rest of the equipment is supplied by Huawei. According to the Angolan authorities, 17 more centres will be built in the same number of provinces for the same purpose. These additional centres ensure coverage of the entire country. Comparative analysis should recognize that numerous countries have similar institutions to help fight crime, articulate medical and fire emergencies, monitor traffic, prevent, and combat crime. Considering the group that governs Angola, it is easy to imagine the purpose for which this institution was created. According to Carlos Albino, commissioner of the National Police, the CISP will function as a command and management body for the force's operations, which will bring together different bodies from the Ministry of the Interior, the Armed Forces, and the External and Internal Intelligence Services. The new security system will be connected to a digital platform that will allow a more efficient communication, through the placement of cameras on public roads in strategic areas, with emphasis on the critical points already identified (Domingos da Cruz, 2022)

Regarding Zambia there is, too, an enormous amount of discussion about China's involvement in electronic surveillance is taking place. Sarah Chiumbu (2021) wrote a thorough report about China's digital infrastructure support of surveillance in Zambia. From the fact that China funds the Smart City initiative, and Huawei and ZTE implemented it under the China Zambia Security Cooperation, Chiumbu argues that "various technologies and Internet of Things (IoT) devices to improve policing and security efforts" were established by Huawei as the 24-hour Close Circuit TV (CCTV), putting cameras "in strategic places and along main roads in Lusaka, including public markets and bus stops" (2022, p. 5).

Based on accusations from digital rights organisations, Chiumbu notes that using Chinese technology in flag-projects, such as Smart City, hides "the selling surveillance technologies to African governments and helps to undermine human rights in these countries" (2021, p. 5). Chiumbu forcefully concludes that, "like many countries in Africa, Zambia mainly uses Chinese surveillance technology made possible by the ease of access, cost, and increased foreign direct investment (FDI) from the Belt and Road Initiative (BRI). There are fears that the entanglement of the Chinese state and its vast array of technology companies in Zambia is promoting the emergence of a surveillance culture" (Chiumbu, 2021, p. 5).

In his interview, Domingos da Cruz considers that the presence of foreign personalities and companies participating in the digital surveillance sector can be seen in two dimensions. First, it obeys a logic of supply and demand. In this sense, we are facing the action of globalisation and capital that circulates on a global scale. Secondly, in the case of governments supporting African regimes, we are facing a game of geostrategic influence and struggle for interests in Africa, as the continent is, again, object of interest from the great powers, once more in a fight for predominance. Its raw materials, ever growing population and vastly unexplored swathes are drivers of greed and intercontinental strife. Also, alternative governance experiments for the democratic-liberal pro market model appear to appeal to those who search for it.

Chapter 3: A brief analysis of relevant actors in SADC surveillance

China, European countries, Israel, the USA, Russia and multilateral organisations such as the European Union are mentioned by Privacy International to be the major providers of surveillance worldwide. They have listed 5 major forms which the surveillance mechanism comes[9]:

- Direct equipping of foreign intelligence and security forces
- Training of foreign intelligence and security forces
- Financing of their operations and procurement
- Facilitating of exports of surveillance equipment by industry
- Promoting legislation which enables surveillance

Through the various interviews and document analysis we have carried out, it is possible to roughly conclude how each of these actors influence surveillance in countries such as Zambia, Mozambique and Angola, taking into account the most frequent forms of surveillance which predominate.

The table below summarises the cross analysis of the actors in the three countries analysed.

9 https://privacyinternational.org/challenging-drivers-surveillance

		Zambia		Angola		Mozambique	
	Forms of surveillance mechanisms	**Yes/No**	**Providers**	**Yes/No**	**Providers**	**Yes/No**	**Providers**
1	**Direct equipping of foreign intelligence and security forces**	Yes	US[10]	Yes	China/ Israel	Yes	China[11]
2	**Training of foreign intelligence and security forces**	Yes	China, Israel	Yes	Israel, China and Russia	Yes	China
3	**Financing of their operations and procurement**	Yes	China, Israel[12]	Yes	China	–	–
4	**Facilitating of exports of surveillance equipment by industry**	No	–	Yes	Huawei (China)	Yes	China
5	**Promoting legislation which enables surveillance**	No	–	Yes	Not specified	Yes	Not specified

10 https://mg.co.za/opinion/2022-06-30-is-the-us-establishing-a-military-base-in-zambia/
11 http://www.connectingtomocambique.com/chinese-group-huawei-plans-to-provide-urban-security-solutions-to-mozambique/
12 https://diggers.news/opinion/2021/03/01/dont-let-china-israel-steal-state-intelligence-through-technology-investments/

USA – there are credible reasons to believe that the US is entering Zambia as it has announced its intention to "direct equipping of foreign intelligence and security forces" (Mulunga, 2022). This hypotheses occurs because in April, "the United States Africa Command (Africom) announced that it had set up an office in the USA Embassy in Lusaka, Zambia" (Prasha, 2022).

China – besides being involved in the training process for the use of ICTs in vital telecommunications infrastructure, especially those considered critical for electronic surveillance, China is indicated in several studies and reports as being the financier and installer of mass surveillance equipment, through the installation of cameras and data centres in several countries in the region. In all three, China is listed as a key international promoter. In Zambia, Angola and Mozambique, China is mentioned as the main supplier of electronic surveillance equipment, through its technological company Huawei, and the installation of equipment for the transformation of Lusaka into a safe city was carried out with Chinese technological investments; In Angola, specifically, the Integrated Security Centre of Benguela was fully funded and installed with the support of China, through business and technology partners such as Huawei; in Mozambique, Huawei has been providing surveillance technology solutions since 2015 (Diggers, 2021; Freedom House 2022; Tatiana, 2020). Both in Mozambique and Angola, Huawei, besides installing its equipment in the telecommunications networks, has memoranda of understanding with local operators to train their engineers to operate the technologies installed in the respective countries.

Training of foreign intelligence and security forces in Mozambique - In June 2016, the Huawei Technologies Group, announced that would strengthen its presence in Mozambique through increasingly advanced training in information and communications technology. Cited by Mozambican daily newspaper Notícias, Huawei said the initiative is being taken in cooperation with the Ministry of Labour, Employment and Social Security, called "Mozambican Seeds for the Future" (Club of Mozambique, 2016). In 2021, Huawei Technologies Co. Ltd of China given about 150 civil servants in Mozambique a course of training in information and communication technology (Forum Chine, 2021). Huawei has been a main promoter of actions that affect the communications sector in Mozambique. In 2015, Chinese group Huawei said that was able to provide technological solutions to ensure safety in some of Mozambique's cities.[13] Chinese are also facilitating of exports of surveillance equipment by industry in Mozambique. In May 2026, Mozambicans learned that their government has been "listening to [their] telephone calls, reading [their] text messages (by SMS, email, WhatsApp, Viber…) and monitoring [social media activity] and Internet sites that they visit." News report Global Voices also described how authorities intercepted and monitored communications between Mozambican citizens using a technical system that was reportedly built by ZTE Corporation, a Chinese company (Tsandzana, D & Anderson, 2016). It was revealed that the system, which has access to all voice communications and data passing through fixed and mobile phone networks, is managed by the military command which facilitates the process. Interceptions do not need prior judicial authorization, much less the agreement of the telecommunications companies. The system also conducts tracking of all communications via email or social networks (idem).

Russia – even without direct references, our interviewees, especially in Angola and Mozambique, show strong relations between Mozambique and Russia, which has an influence on political and legislative processes on surveillance. On the other hand, in Mozambique, in the early stages of the fight against insurgency, direct use was made of technology and of Wanger mercenaries with strong connections to the Russian government.

13 http://www.connectingtomocambique.com/chinese-group-huawei-plans-to-provide-urban-security-solutions-to-mozambique/

Israel – has been referred to in Zambia and Angola as facilitating surveillance, especially with the provision of technology for surveillance, through the technology company NSO Group. As Freedom House reports on Angola: "In June 2020, reports emerged that Angolan intelligence services had purchased Pegasus spyware, which allows users to compromise devices and monitor communications, from the Israeli technology company NSO Group. Pegasus was known to have abused vulnerabilities in WhatsApp, the dominant messaging app in Angola that is widely used by journalists, activists, and opposition politicians. A 2018 Haaretz investigation found that an unnamed Israeli company had sold social media monitoring software to the Angolan government". In Mozambique, Israel has related to the provision of military equipment for surveillance in the context of counterterrorism in the northern province of Cabo-Delgado (The Defense Post, 2022).

Conclusions

Our main conclusion is straightforward. There would be no electronic surveillance in southern Africa without the strong participation of international actors that provision and train local operators in surveillance technology. Our research emphasized the role of private international providers. These actors come from several countries, such as the United States, China and Israel. Although in what can be called Western or pro-Western countries, the task of identifying the location of each of the specific companies that provide services or technologies is difficult, given the multinationalization of corporations. We found an Israeli company belonging to a Japanese group (Sun), or another supposedly Israeli company operating through a Bulgarian subsidiary (Circle/NSO). Therefore, we conclude that the export regulations are not so important as at first instance could appear, at they would be easily circumvent.

The Chinese case is simpler. It is easy to assign companies to China. However, here the problem is on another level. It is about the connection of these companies with the Chinese security apparatus.

In recent years, in almost all SADC countries, cases of surveillance have been reported, mainly to limit civic and political freedoms by targeting journalists, activists of civic organisations and opposition party politicians, especially in countries with dominant party systems. Several of the problems are situated in the media space with governments attempting to over-control the work of journalists, leading to various types of abuses, such as passing diverse legislation of control over civic space, harsh control of journalists and activists and surveillance of investigative journalists, which has been a key reason for the regression of the environment of freedoms of expression in many of the countries.

Laws that promote an environment of surveillance and excessive control of freedoms make this possible. Data protection and cybersecurity laws are used to watch and repress freedom of expression and the right to information. In other cases, the existence of legislation prohibiting surveillance or protecting freedoms is forgotten, and surveillance happens without any legal worries, as the ones that disregard the law are the same that should enforce it.

Regarding the specific international drivers of surveillance in southern Africa, we investigated several countries. They could be considered structural examples of general trends in the area.

Our report found that the US was to be directly mentioned at least in Botswana, where there are references to Access Data and a FTK that the

police force used to extract information from electronic devices, including those that were locked. The FTK is a computer forensics software made by the Access Data corporation and scans a hard drive looking for various information. This company is owned by Exterro Inc., a company based in Oregon, US, partially owned by an equity fund (Leeds Equity Partners which should have investors from around the globe, which pinpoint our argument about the multinationalistaion of this corporations).

Huawei, a Chinese corporation, is mentioned more often these days. Apparently, Huawei has certain obscure links to the Chinese Security system and the USA considers it a danger to the security of communications in other countries as South Africa. (Swart, 2020). The Biden administration, in 2021, designated five Chinese technology firms as an "unacceptable risk" to American national security, in which Huawei stands out. At the same time, President Joe Biden's government has imposed restrictions on some Huawei suppliers on the export of items intended for use on 5G networks. Washington assumes that Beijing can use Huawei equipment to spy on US residents. To countervail Huawei´s influence is currently a part of American foreign policy.

In our research, there is an enormous amount of discussion about China's involvement in Angola and Zambia. That is happening in relation to China's digital infrastructure support of surveillance in Zambia. From the fact that China funds the Smart City initiative, and Huawei and ZTE implemented it under the China Zambia Security Cooperation, it is argued that various Chinese technologies were used to improve policing and security efforts mounted by Huawei. However, the frontiers between policing and unlawful vigilance are too blurred to achieve satisfactory conclusions. As it relates to China, there is a wall of opacity that tends to difficult research work.

Contrary to China, the role of Israeli branded companies is extremely noticeable. With regard to the identified activities of various Israeli private companies in the operationalisation of large surveillance operations in Africa. The role of Israeli private companies and citizens in surveillance in southern Africa is manifest, and the implications of such actions should be discussed.

In the end, private international drivers of surveillance are having a consistent and perilous role in developing sophisticated operations of vigilance in southern Africa which encroach on civil rights, but a lot more research is needed to clarify the extent of each intervention.

Direct interviews

Interview member of the Angolan intelligence services (retired/Anonymous)-September 2022

Interview Jean-Jacques Wondo (DRC) – September 2022

Interview Domingos da Cruz (August 2022)

Interview Israeli Human Rights activist (July 2022)

Interview Richard Mulunga (Blogger of Zambia) – September 2022

Interview Dércio Tsandzana (Mozambique) – September 2022

Interveiw Armando Nhantumbo (Mozambique) – September 2022

References

Abdulrauf, L.A. 'The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa'(2018) 18 African Human Rights Law Journal 365-391

ACLED, 2022, Wagner Group Operations in Africa. Civilian Targeting Trends in the Central African Republic and Mali, https://acleddata.com/2022/08/30/wagner-group-operations-in-africa-civilian-targeting-trends-in-the-central-african-republic-and-mali/

Balule, T. B. (2021, November). *Surveillance of digital communications in Botswana: An assessment of the regulatory legal framework*. Media and democracy. https://www.mediaanddemocracy.com/

Biddle, S., & Desmukh, F. (2016, December 8). *Phone-cracking Cellebrite software used to prosecute tortured dissident*. The Intercept. https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/

Black Cube. (2010). https://www.blackcube.com/

Bulelani Jili, 2020, The Spread of Surveillance Technology in Africa Stirs Security Concerns, Africa Center for Strategic Studies, https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/

Chiumbu, S. (2021). *Chinese Digital Infrastructure, Smart Cities and Surveillance in Zambia*.

Club of Mozambique (2016). *Huawei Tecnologies trains technical staff from Mozambique*. https://clubofmozambique.com/news/huawei-technologies-trains-technical-staff-from-mozambique/, accessed in 20 September, 2022

Conecting to Mozambique. *Chinesse groyo hyawei plans to proived urban security solution to Mozambique*. http://www.connectingtomocambique.com/chinese-group-huawei-plans-to-provide-urban-security-solutions-to-mozambique/, accessed in 20 September, 2022.

Costa, T. (2020). *Inaugurado Centro Integrado de Seguranca Publica em Benguel*a. https://www.verangola.net/va/pt/112020/Defesa/22694/Inaugurado-Centro-Integrado-de-Segurança-Pública-em-Benguela.htm

Cotterill, J., & Croft, J. (2021, March 29). *Africa's richest woman says she was targeted in 'personal vendetta'*. Financial Times. https://www.ft.com/content/5ce9aed7-7a8c-4c38-b18f-d88e8bd5fe86

Diggers (2021). *Don't let China, Israel steal State intelligence through technology investments*. https://diggers.news/opinion/2021/03/01/dont-let-china-israel-steal-state-intelligence-through-technology-investments/, accessed in 20 September, 2022

Exterro. (2022). https://www.exterro.com/

Fasanotti, F. S. (2022, February 8). *Russia's Wagner Group in Africa: Influence, commercial concessions, rights violations, and counterinsurgency failure*. Brookings Institute. https://www.brookings.edu/blog/order-from-chaos/2022/02/08/russias-wagner-group-in-africa-influence-commercial-concessions-rights-violations-and-counterinsurgency-failure/

FES & MISA (2018). *African Media Barometer: Mozambique – 2018*. Windhoek: FES. https://www.misa.org.mz/index.php/publicacoes/relatorios/relatorio-2008/101-barometro-africano-dos-media-mocambique-2018. Accessed on October, 29, 2020.

Forum China PLP (2021). *Mozambican civil servants complete Huawei course on ICT*. In https://www.forumchinaplp.org.mo/mozambican-civil-servants-complete-huawei-course-on-ict/#

Freedom House (2021). Freedom on the Net 2021: Angola. https://freedomhouse.org/country/angola/freedom-net/2021, accessed in 20 September, 2022

Gadi, P. (2022, February 15). *It's not about privacy: NSO scandal shows risk of rogue intel forces*. Haaretz. https://www.haaretz.com/israel-news/tech-news/.premium-it-s-not-about-privacy-nso-scandal-shows-risk-of-rogue-intel-forces-1.10613181

Gwagwa, A. (2017). *Digital media: An emerging repression battlefront in Angola*. Nairobi, Kenya: Centre for Intellectual Property and Information Technology Law, Strathmore Law School Strathmore University. https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations

Leeds Equity Partners. (2021). https://www.leedsequity.com/

Links, F (2021a). *Data retention regulations eradicate anonymity*. Action, https://action-namibia.org/data-retention-regulations-eradicate-anonymity/

Links, F. (2021b). *State surveillance abuse threat looms large*. Action, https://action-namibia.org/state-surveillance-abuse-threat-looms-large/

Mare, A. (2021). *Communication surveillance in Namibia: An exploratory study*. Media and Democracy. https://www.mediaanddemocracy.com/

Mguni, M. (2022). *Controversial "spy bill" stokes rare public debate on civic surveillance*. Mmegionline, https://www.mmegi.bw/features/controversial-spy-bill-stokes-rare-public-debate-on-civic-surveillance/news#,

MISA (2021). *Southern Africa Press Freedom Report 2010–2020*. Harare: MISA Zimbabwe.

MISA (2022). *Proposta de Lei "Anti-Terrorismo" restringe Liberdades de Expressão e de Imprensa em Moçambique*, https://www.misa.org.mz/index.php/destaques/noticias/141-proposta-de-lei-anti-terrorismo-restringe-liberdades-de-expressao-e-de-imprensa-em-mocambique.

MISA Zimbabwe. (2020). *Government asked to enact Cybersecurity Bill in line with continental benchmarks*. https://zimbabwe.misa.org/2020/07/16/government-asked-to-enact-cybersecurity-bill-in-line-with-continental-benchmarks/

Moyo, H. (2022). *Lesotho's cyber law not well thought-out, potentially violates human rights: Analysts*. Lesotho Times. https://lestimes.com/lesothos-cyber-law-not-well-thought-out-potentially-violates-human-rights-analysts/

MPDP. (n/d). https://www.mediaanddemocracy.com/.

Musole, T. M., & Rwabashi, J.-P. M. (2021). *Digital surveillance and privacy in DRC: Balancing national security and personal data protection*. Media and Democracy. https://www.mediaanddemocracy.com/.

Ndlela, D. (2020a). *Privacy violations fears grow as govt sets surveillance cameras in cities*. The Standard. https://www.thestandard.co.zw/2020/06/21/privacy-violations-fears-grow-govt-sets-surveillance-cameras-cities/

Ndlela, D. (2020b). *Zimbabwe's new cyber law to target online government and military critics*. The Standard. https://thestandard.newsday.co.zw/2020/07/12/zimbabwes-new-cyber-law-to-target-online-government-and-military-critics/?amp=1

Nhanale, E. (2021). *Electronic surveillance in Mozambique: The risks and suspicions in a context of authoritarianism and military conflict*. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_04_2021_electronic_surveillance_ mozambique_masterset.pdf. Accessed on February 9, 2022.

Prashad, Vijay (2022). *Is the US establishin a military base in Zambia?*. https://mg.co.za/opinion/2022-06-30-is-the-us-establishing-a-military-base-in-zambia/, accessed in 20 September, 2022

Privacy International, 2021, Huawei and Surveillance in Zimbabwe, https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe

Privacy International, s/d, Challenging the Drivers of Surveillance, https://privacyinternational.org/challenging-drivers-surveillance

Robinson, J. A. (2013). *Botswana as a role model for country success*. In A. Fosu (Ed.), Achieving development success: Strategies and lessons from the developing world, (pp. 186-203). Oxford.

Sikhakhane, N. (2022). *Activists under threat from surveillance*. New Frame. https://www.newframe.com/activists-under-threat-from-surveillance/

Skelton, S. K. (2021). *Illegal state surveillance in Africa 'carried out with impunity.'* Computer Weekly. https://www.computerweekly.com/news/252508766/Illegal-state-surveillance-in-Africa-carried-out-with-impunity

Snowden, E. (2019). *Permanent record*. MacMillan.

Swart, Heidi, 2020, Part One: Are South Africans safe with Huawei? It's all about the risk, https://www.dailymaverick.co.za/article/2020-03-05-part-one-are-south-africans-safe-with-huawei-its-all-about-the-risk/

The Defense Post, 2022. *Israeli System Downs ISIS Drones In Mozambique*. In https://www.thedefensepost.com/2022/03/10/israeli-counterdrone-mozambique/

The Economist. (2022). *A new low for global democracy: More pandemic restrictions damaged democratic freedoms in 2021*. https://www.economist.com/graphic-detail/2022/02/09/a-new-low-for-global-democracy

Tsandzana, D & Anderson, L (2016). *The government of Mozambique is "spying on its Citizens", according to @Verdade*. https://advox.globalvoices.org/2016/05/16/the-government-of-mozambique-is-spying-on-its-citizens-according-to-verdade/

Verde, R. (2021). *Israeli involvement in electronic surveillance in Angola: A step towards transparency or the sophistication of illegal practices?* Media and Democracy. https://www.mediaanddemocracy.com/

Walters, J. (2018). *'Shithole' remark by Trump makes global headlines – but it doesn't quite translate*. The Guardian. https://www.theguardian.com/us-news/2018/jan/12/trump-shithole-countries-lost-in-translation

Media Policy and Democracy Project

The Media Policy and Democracy Project (MPDP) was launched in 2012 and is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg (UJ). The MPDP aims to promote participatory media and communications policymaking in the public interest in South Africa.

Visit mediaanddemocracy.com for more information.
This report was supported by a grant from Luminate.