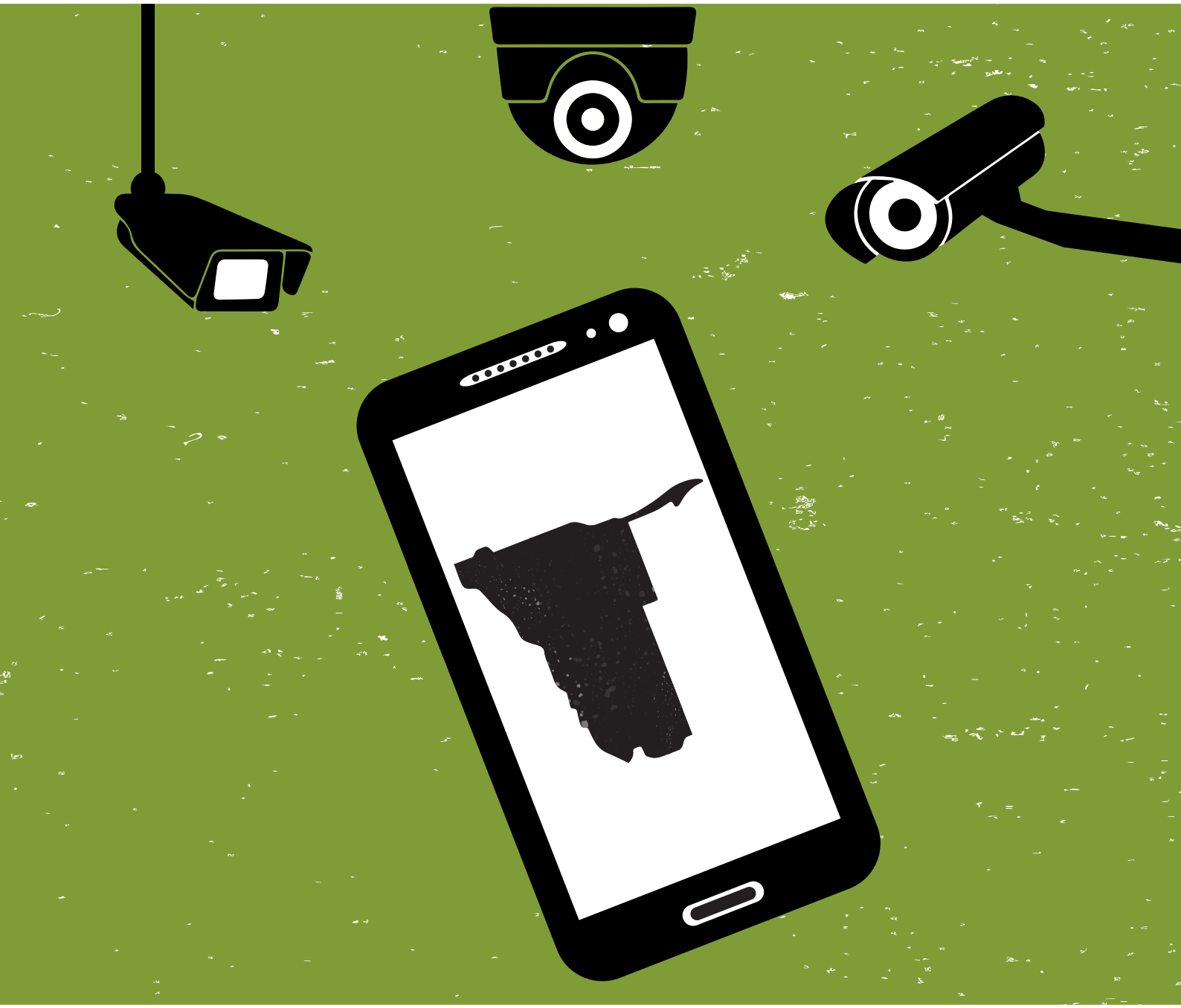
Communication Surveillance in Namibia: An Exploratory Study



Admire Mare

Communication Surveillance In Namibia: An Exploratory Study

A report compiled by Admire Mare

 We would like to thank Privacy International, who provided funding for this project through a grant they received from the Ford Foundation under the 'Security on our own terms – developing global South leaders in the field of cybersecurity' project.

November 2019

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

List of Acronyms

4IR	Fourth Industrial Revolution
ADSL	Asymmetric Digital Subscriber Line
ANC	African National Congress
AU	African Union
BTI	BertelsmannStiftung
CBD	Central Business District
CCTV	Closed-circuit Television
CRAN	Communications Regulatory Authority of Namibia
DCN	Democratic Coalition of Namibia
DPA	Data Protection Authority
ETC	Electronic Transactions and Cybercrime
GCHQ	Government Communications Headquarters
LAC	Legal Assistance Centre
LaRRI	Labour Research and Resource Centre
LPM	Landless Peoples' Movement
IMSI	International Mobile Subscriber Identity
IPPR	Institute of Public Policy Research
MAG	Monitor Action Group
MICT	Ministry of Information and Communication Technology
MISA	Media Institute of Southern Africa
MTC Namibia	Mobile Telecommunications Limited Namibia
NBC	Namibia Broadcasting Corporation
NEFF	Namibia Economic Freedom Fighters
NamRights	Namibian Society for Human Rights
Nampol	Namibia Police Force
NID	Namibia Institute for Democracy
NIGF	Namibia Internet Governance Forum
NMT	Namibia Media Trust
NCIS	Namibia Central Intelligence Services
NSA	National Security Agency
PDM	Popular Democratic Movement
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
SADC	Southern Africa Development Community
SIG	Single Internet Gateway
SIM	Subscriber Identification Module
SWAPO	South West Africa People's Organisation
UN	United Nations
UNHRC	United Nations Human Rights Committee
UDF	United Democratic Front

Table of Contents

1. **Executive Summary** 1

2. **Introduction and Background of the Report** 2

3. **Research Context** 6

4. **Methodological Approach** 10

5. **Preliminary Findings** 11

6. **Conclusion and Recommendations** 26

7. **References** 32

1. Executive Summary

This mapping study sought to explore the emerging practices and cultures around communication surveillance in Namibia. The study attempts to shed light on the surveillance technologies used to spy on people, their capacities, the targets of surveillance and the ways in which civil society organisations are pushing back against the normalisation of surveillance in post-apartheid Namibia.

It endeavoured to find out if Namibia can be characterised as a "surveillance state" with the capacity to use data-driven surveillance technologies to monitor the everyday lives of ordinary citizens and perceived political 'enemies'. The study will also focus on the following areas:

- Namibia and the global trade in data-driven surveillance tools, focusing particularly on the growing influence of China;
- The adequacy of oversight of these forms of surveillance;
- Capabilities of the institutions undertaking these forms of surveillance and their uses;
- Building the capacities of civil society to hold these institutions accountable, through research and investigative journalism.

Deploying a combination of qualitative policy analysis, document analysis and in-depth interviews with key informants drawn from professional journalists, civil society, Windhoek City Police and regulatory authorities, the study revealed that there are a number of reasons to believe that unlawful communication surveillance is occurring in Namibia.

These reasons include regulatory/institutional and reported activities of unlawful surveillance and concerning practices. As this report will show, some of institutional and concerning practices consist of the controversial part 6 of the Communications Act of 2009[1] (more information about this clause will be discussed later in the report); the role of Chinese telecommunication giants especially ZTE and Huawei Technologies in the Namibian telecommunications sector; the acquisition of surveillance technologies; the government's monopoly in the telecommunications sector; lack of regulatory independence on the part of Communications Regulatory Authority of Namibia (CRAN); the push by the government for the roll-out of the Single Internet Gateway system; the reported surveillance of Members of Parliament; the existence of interception centres; the absence of judicial authorisation and transparent oversight mechanisms over the intelligence agencies; the proposed Electronic Transactions and Cybercrime Bill; the lack of a comprehensive data protection law and calls for mandatory Subscriber Identification Module (SIM) card registration. It is clear from the foregoing that some of these are reasons for surveillance, while others are the symptoms/consequences.

Thus, whilst the technological surveillance capabilities of Namibia remain largely unknown and/or lacking concrete evidence, the fact that the country has acquired a variety of surveillance technologies including International Mobile Subscriber Identity (IMSI) catchers, sophisticated surveillance video cameras and other related gizmos raises serious concern with regards to how these technologies are being deployed, bearing in mind that part 6 of the Communication Act of 2009 is still not yet in operation. Interviews with various key informants in Namibia revealed that the targets of communication surveillance are likely to include investigative journalists, opposition parties, factions within the ruling party and members of the civil society organisations.

One of the major findings of this study was that Namibia does not have adequate oversight mechanisms to enable legitimate, proportionate and necessary communication surveillance in the digital age. The current legislative regime as evidenced by the Namibia Central Intelligence

1 It regulates communications surveillance by the Namibian government.

Services Act of 1997 and the Communications Act of 2009 (especially part 6, section 70-77) is not fit for purpose. A set of recommendations for the government, the Parliament, civil society organisations, and research institutions is detailed in the final section of the report.

2. Introduction and Background of the Report

The world has witnessed an unprecedented trend towards the accumulation of digital data, computerisation and automation of everyday life. It is no wonder that privacy is fast becoming "a relic of the pre-internet age" (Big Brother Watch, 2018). On the one hand, platform companies are profiting from tracking, analysing and quantifying every 'consumer' while on the other hand, authoritarian and democratic states are building "surveillance societies[2]" (Lyon, 2001). The rapid emergence of new surveillance technologies is being matched by their fast and often lawless adoption by private companies and the state (Big Brother Watch, 2018). These processes often described as part of the so-called "Fourth Industrial Revolution[3] (4IR) or the "data-driven economy" has also heralded both mass and targeted forms of communication surveillance. Communication surveillance encapsulates a broad range of activity that implicates the privacy and expressive value inherent in communications networks (Human Rights Watch, 2014). It includes not only the actual reading of private communication by another human being, but also the full range of monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, or arises from a person's communication in the past, present, or future. Aided by new digital media technologies, communication surveillance has become very pervasive and fluid in nature. These pervade every aspect of daily life, from our online shopping, browsing and social activities, to the ways we move through public spaces and transportation systems under the watchful eye of closed-circuit television (CCTV) cameras (Wahl Jorgensen, Bennet, Hintz and Dencik, 2017).

Furthermore, Dencik (2015) argues that we are living in a state of "surveillance realism" where we "accept it as an inevitability of our world" and do not question or contest it. Surveillance has always been part of the construction of the nation state. Different regimes of surveillance have been deployed since time immemorial by nation states to control and discipline populations. However, there is something new about the kinds of surveillance being incorporated in everyday life in the era of 'datafied society[4]' (van Dijck, 2014). Security forces can watch and track citizens without suspicion, increasingly using algorithms fed with personal information and data scraped from the internet and social media to construct 'suspicion', assert 'risk', or even predict crime (Ferguson, 2017). Facial recognition cameras have crept onto our streets, making border style security and frequent identity checks a norm (Big Brother Watch, 2018).

In an investigative report published by the French newspaper Le Monde[5] in 2018, China, which also paid and built the computer network at the African Union (AU) headquarters in Addis Ababa, Ethiopia, allegedly inserted a backdoor that allowed it to transfer data (Dahir, 2018). Chinese telecommunication companies (ZTE and Huawei) were implicated in this spying scandal. The spy scandal was only discovered in January 2017 (five years after the building was commissioned) when technicians noticed that between midnight and 2am every night, there was a peak in data usage even though the building was empty. It was also discovered that AU's confidential data was being

2 A society organised around the collection, recording, storage, analysis and application of data on individuals and groups by state and corporate actors (Lyon, 2001).

3 The Fourth Industrial Revolution is characterised by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human (Schwab, 2016).

4 The gathering of extensive data about all of us is pervasive, opaque, yet central to the functioning of consumer capitalism.

5 http://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

copied on to servers in Shanghai. This incident further sheds light on the vulnerabilities inherent in digital communication technologies in the age of "surveillance society" (Lyon, 2001) and "surveillance capitalism" (Zuboff, 2018).

Furthermore, recent media reports that WhatsApp (one of the most popular mobile instant messaging app in Namibia and the global south) was targeted for surveillance purposes further raises concern about the safety of the data in the hands of global and local internet intermediaries. Hackers were able to remotely install surveillance software on phones and other devices using a major vulnerability in the messaging app (Lee, 2019). The vulnerability allowed attackers to install malicious code on iPhones and Android phones by ringing up a target device. As Lee (2019) points out, the code could be transmitted even if users did not answer their phones and a log of the call often disappeared. The spyware was developed by NSO Group (an Israeli cybersecurity and intelligence company). Interestingly, WhatsApp promotes itself as a "secure" communications app because messages are end-to-end encrypted, meaning they should only be displayed in a legible form on the sender or recipient's device (Lee, 2019). While the revelation is said to have enabled the company to fix the flaw that allowed this attack to take place, WhatsApp has not indicated whether the update removes any spyware that has already infected a compromised device.

Figure 1: Differences between mass and targeted communication surveillance

Mass versus targeted communication surveillance

Mass surveillance: This is the subjection of a population or significant component of a group to indiscriminate monitoring. Any system that generates and collects data without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance and it increasingly involves the generation, collection, and processing of information about large numbers of people.

Targeted surveillance: This is surveillance directed at particular individuals. Targeting methods include the interception of communication and the use of communication data.

Source: Right2Know Campaign. 2016. The Surveillance State: Communications surveillance and privacy in South Africa.

In the recent past, Edward Snowden's revelations about the extensive surveillance programmes of the National Security Agency (NSA) in the United States and the Government Communications Headquarters (GCHQ) in the United Kingdom, revealed that intelligence agencies routinely gather vast amounts of data about our activities (Wahl Jorgensen, et al., 2017). Snowden also showed that surveillance occurred via the interception of data shared on the internet, hacking into computer systems and compromising security levels. It also entailed the bulk collection of everyone's data as well as targeted surveillance of governments, companies and civil society organisations (Wahl Jorgensen, et al., 2017). The revelations indicated that the intelligence agencies accessed information gathered by Facebook, Google, Apple and other technology companies (Fidler, 2015). Because of its nefarious nature, citizens across the globe are increasingly coming to accept the ubiquity and pervasiveness of surveillance as part and parcel of everyday life (Bauman and Lyon, 2013).

The Snowden revelations, which uncovered extensive and indiscriminate surveillance efforts worldwide, raised substantial legal and policy questions. In some progressive states, the revelations helped to kick-start discussions around the need for reform of data protection and privacy laws as

well as the rebooting of archaic intelligence and security services legislation. There have been global calls for nation states to align their new laws with the International Principles on the Application of Human Rights to Communications Surveillance (also known as the Necessary and Proportionate Principles). Whilst Snowden and WikiLeaks revelations provided the world with sneak previews of the nature, extent and metamorphosis of communication surveillance in the global North, there is little that is known about this phenomenon in global South (Duncan, 2018; Mare, 2016; Privacy International, 2017; Links, 2018; Tendi, 2016). Significant literature (Duncan, 2018; Hunter, 2016; Mare, 2018) has begun to emerge in South Africa, Zimbabwe and Mauritius highlighting the pernicious effect of communications surveillance. With the exception of media and policy reports (Links, 2018; Privacy International, 2017), there is a dearth of evidence-based information on the state of communications surveillance in Namibia. This exploratory study puts the spotlight on the surveillance technologies used to spy on people, their capacities, the targets of surveillance and the ways in which civil society organisations are pushing back against the normalisation of surveillance in post-apartheid Namibia.

2.1 Rationale for the research project

Research (see for instance, Human Rights Watch, 2014; Duncan, 2017; Mare, 2016) suggests that activists, human rights lawyers, opposition political actors, trade unionists and journalists who work in both democratic and authoritarian environments are more vulnerable to cases of electronic surveillance. For instance, because of the sensitive nature of their communication with research participants, academics need to have privacy of their communication guaranteed as a precondition for academic freedom (Duncan, 2016). They occasionally offer confidentiality to interviewees in the course of research, and may be unable to maintain this ethical duty in the absence of such privacy. Sources of information are the lifeblood of journalism, too; without them, reporting on sensitive topics would become difficult to impossible (Duncan, 2016). Similar to academics, journalists have an ethical obligation to protect sources once they offer them confidentiality, and surveillance erodes their ability to do so (Duncan, 2016). In the same vein, human rights lawyers also need to offer their clients attorney-client privilege to ensure that interactions between them and their clients is an open and robust as possible (Human Rights Watch, 2014). In short, the state has a positive duty to shield activists, human rights lawyers, journalists and academics from unwarranted intrusions into the privacy of their communication (Duncan, 2016). There are no legally-recognised protections for political activists against state surveillance, though, which makes them particularly vulnerable to privacy violations.

Communication surveillance has begun to replace censorship as the weapon of choice for both democracies and repressive regimes intent on silencing and intimidating critical voices (Lyon, 2001). It undermines critical and investigative reporting, which requires confidential communication with sources and, occasionally, the anonymity of authors (York, 2014). Some governments have been implicated in the processes of spying on journalists' emails to identify confidential sources, tracking journalists via their mobile phones and hacking journalists' computers and infecting them with malware (Human Rights Watch, 2014; Dencik, 2015).

This kind of communication surveillance makes it difficult for the media to challenge powerful institutions, bear witness and represent the public interest. As York (2014) observes, surveillance does not only impede journalists' ability to do their work but also endangers the safety of their news sources. This breeds a culture of "chilling effects", which has been defined as the idea that laws, regulations, or state surveillance can deter people from exercising their freedoms or engaging in legal activities on the internet have taken on greater urgency and public importance (Penney, 2017). As Schauer (1978: 689) observes, a "chilling effect" is at its

core an "act of deterrence" and the fear, risk, and uncertainty built into laws, regulations, and the legal system more generally, can deter people from exercising their rights. Writing about concerns about state surveillance and data gathering by private companies, Solove (2006: 487) argues that these practices can create an atmosphere of "risk" and self-censorship, a kind of society-wide chilling effect comparable to "environmental harms" or "pollution". In order to explore the chilling effects of government surveillance measures, Sidhu (2007) conducted a survey of Muslim-Americans to determine if and to what extent Muslims in the United States, concerned that the government may track their online movements, have changed their use of the Internet after 9/11. The survey's results indicate that an overwhelming majority of polled Muslim-Americans believe that the U.S. government monitors their post-9/11 Internet activities, although only a limited segment of the Muslim-American population has changed its online behavior (Sidhu, 2007). Muslim-Americans do not only believe the government monitors their routine activities, but that such concerns have translated into actual changes in daily behavior.

Data-driven surveillance is notoriously difficult to detect; yet if misused, it can enable wide-scale repression of civil society and journalists. This is partly because of its over-reliance on back-end technologies and other insidious capabilities. Such surveillance was used massively during the Arab Spring, and there is evidence of surveillance having been central to the repression of protests in Southern Africa (Gerbaudo, 2013). There is also reported evidence of countries such as China supplying surveillance tools to Southern African governments (such as Mozambique and Zimbabwe), with no real evidence of whether the exporters have considered whether they will be used for legitimate public safety and national security purposes, or to enable human rights abuses. For instance, In March 2018, the Zimbabwean government signed a strategic partnership with the Gunagzhou-based startup CloudWalk Technology to begin a large-scale facial recognition program throughout the country (Chutel, 2018). The agreement, backed by the Chinese government's Belt and Road Initiative, will see the technology primarily used in security and law enforcement and will likely be expanded to other public programmes (Chutel, 2018). This lack of regard for human rights is unsurprising, as export controls of these surveillance tools are still lax.

Many countries in Southern Africa have been expanding their surveillance capabilities as part of a growing wave of authoritarianism in the region. Examples include the shrinking democratic space in Zimbabwe, Zambia and Mozambique, where media reports have shown that authoritarian leaders have resorted to deploying surveillance technologies to control and discipline citizens (Mare, 2018; Tendi, 2016). In South Africa, under the leadership of Jacob Zuma, surveillance was also used against political enemies with the African National Congress (ANC) (see Duncan, 2014).

Another major exporter of surveillance tools, like the United Kingdom, has exported highly-invasive international mobile subscriber identity catchers (IMSI-catcher) to Namibia (see Links, 2018), and Israel and South Africa also appear to be active in exporting to the region (Mare, 2016). Deep Packet Inspection software has been detected in Zambia, which was also identified as a major regional surveillance hub in documents leaked by former NSA contractor Edward Snowden (Greenslade, 2013; Greenwald, 2014). Leaked emails from the Italian surveillance firm Hacking Team also revealed that the company might have sold its sophisticated spyware known as Remote Control System (RCS) to the Zambian authorities (Gallagher, 2015). This is because there were leaked emails of their meeting.

As Wahl-Jorgensen, et al (2017) observe, the emergence of a "surveillance society" raises important questions around new threats to journalistic freedom and political dissent; the responsibilities of media organisations and state actors; the nature of journalists' relationship to the state; journalists' ability to protect their sources and data; and the ways in which media coverage shape public perceptions of surveillance.

Indications are that Namibian state security has had dealings with at least two – Gamma Group and HackingTeam – of the 'Corporate Enemies of the Internet' in recent times (Links, 2018). Yet, in spite of growing reports about the state surveillance capabilities in Namibia, civil society has not developed a coordinated response.

The rationale of this project is to begin a process towards building civil society and journalistic capacities to map these trends and, where necessary, to hold the main surveillance actors to account.

3. Research Context

On March 21, 1990, Namibia achieved independence. This opened a new chapter in the country's history and paved the way for a wide-ranging transformation of the country under a legitimately elected government (BTI Report, 2018). Since 1990, Namibia has been a multiparty democracy, with normative values enshrined in a liberal constitution that protects civil rights and liberties (including press freedom). But certain clauses in the constitution have limited property rights (BTI Report, 2018). Hence, the political freedoms went hand in hand with a market economy, which to a large extent protected the economic status quo after independence regarding property rights. This made it more difficult to promote social change and the redistribution of wealth (BTI Report, 2018). On the other hand, it ensured stability and trust enabling the government to pursue the reconciliation of antagonistic interests inherited from the apartheid era. Namibia's government hence secured a relatively high degree of social capital both at home and abroad (BTI Report, 2018).

Namibia, a middle-income country with a total population of more than 2 million, has been singled out by the United Nations Human Rights Committee as one of the many Southern African countries which is engaging in communication surveillance. There are several factors that explain this authoritarian turn in post-apartheid Namibia. Like its neighbours (especially Angola, Zimbabwe and South Africa), Namibia is still under the political domination of the liberation war party, the South West Africa People's Organisation (SWAPO). The party has won every parliamentary election by large majorities since 1990. In many ways, the country can be described as a one-party state, given the political domination of the ruling party. With the exception of McHenry Venaani's Popular Democratic Movement (PDM) party, other opposition parties in Namibia are highly ethnicised and too fragmented to be able to dislodge SWAPO from the apex of political power. Opposition parties often lack alternatives and are typically limited to regional-ethnic support (BTI, 2018). SWAPO has been the only relevant political force able to unite the divided country. However, socioeconomic discrepancies over the last 26 years have created a cocktail of problems. Ordinary people in urban areas have begun to question the general direction of the country and the demands for service delivery have become louder and louder. Corruption and lethargic service delivery has galvanized urbanites to start mobilizing against the political hegemony of SWAPO.

Another issue, which has caused several challenges for the government relates to the equal redistribution of land. The Landless Peoples' Movement (LPM) has used the emotive issue to push the government to adopt a more radical approach to the issue. Leaders of LPM are believed to be some of the targets of government monitoring and surveillance given the unequal distribution of the scarce resource in a multi-ethnic society (Links, 2019). The issue of land reform remains a thorny issue, which has in the past triggered regional-ethnic animosities. Minority groups claim that the current land policy advantages the Oshiwambo-speaking majority group, especially in eastern, central and southern Namibia where the Herero, Nama and Damara minorities mainly resident (BTI Report, 2018). These animosities have also been articulated by some within the ranks of the SWAPO

and causing internal party friction. This has resulted in interventions by the president and even the dismissal of a deputy minister over the government's disputed land and resettlement reforms (BTI, 2018).

Namibia remains one of the most unequal societies in the world in terms of income inequality (BTI Report, 2018). Though overall Namibia remains a relatively stable country, social protests and ethnic tensions have increased in recent years (BTI Report, 2018). For instance, in 1999, there was an armed secessionist attacks in Katima Mulilo (Eastern Caprivi). As a result, some ethnic groups in former Caprivi territory are still not content with the SWAPO government. In 2016, there were country-wide protests among affected groups (Nama and Herero) and increased ethnic tensions (BTI Report, 2018). The notion of belonging became a much more discussed matter, which also affected perceptions of the nation-state and its inclusiveness.

Because of the weak opposition parties in Namibia, internal strife within the ruling SWAPO have also been fingered as the reason for increased cases of communication surveillance. In 2005, internal party differences resulted in the establishment of a second break-away opposition party. However, both breakaway parties were short-lived and never able to secure widespread electoral support beyond existing opposition supporters (BTI Report, 2018). The parliamentary elections are proportional and based on party lists, which makes internal party competition an important factor. Consequently, there are always factional battles within the ruling party. For instance, during the last general elections there was a highly publicised tussle between Team Swapo and Team Harambee (Tjitemisa, 2018). Team Harambee was fronted by President Hage Geingob while Team SWAPO had the likes of Jerry Ekandjo and former Prime Minister Nahas Angula. Team Harambee, led by party and state president Hage Geingob, emerged runaway victors at the last party congress, where he faced Jerry Ekandjo and Nahas Angula in the party presidency contest. Murmurs of discontent, capped by allegations of purging, exclusion and, startlingly, election rigging have been going on a year since the last party congress took place.

Despite the factional battles in the run-up to the November 2014 elections, SWAPO secured an absolute majority. During the last general elections the ruling SWAPO party won 53 of the 72 elected National Assembly seats (BTI Report, 2018). Moreover, the party's presidential candidate has always won even more votes than the party in each presidential election since independence. In the last presidential election, Geingob won a record 86% of votes. SWAPO of Namibia is the ruling party and has been since independence in 1990. The Popular Democratic Movement (PDM) is the official opposition, while other political parties represented in the Parliament are the United Democratic Front (UDF), the Democratic Coalition of Namibia (DCN) and the Monitor Action Group (MAG).

Although civil liberties and self-determination are guaranteed for every Namibian in the Constitution, many people continue to live in poverty. The issues of informal settlements and migrants who are believed to 'steal' jobs from locals have dominated electoral issues in the previous elections (BTI Report, 2018). There is growing dissatisfaction amongst the general populace with the lack of policy achievements on the part of SWAPO. Service delivery is skewed and some of the poorest among the 14 regions lack adequate access to health care facilities and educational services (BTI Report, 2018). Efforts to transform the economy, however, have mainly involved increasing access for the new elite to state resources and have not improved pro-poor policy outcomes (BTI Report, 2018).

Namibia has a wide array of civil society organisations. Most of these civic actors work in the area of social activities and issues (e.g., HIV/Aids, gender, health care and education) and have no direct political impact. This does not mean they are not active in the human rights space. Particularly influential human rights NGOs include the Legal Assistance Centre (LAC) and NamRights (formerly Namibian Society for Human Rights), as well as Namibia Media Trust (NMT). Other significant

NGO groups include independent research and advocacy institutions, most prominently the Institute for Public Policy Research (IPPR). Though other NGOs have become less prominent, such as the Namibia Institute for Democracy (NID) and the Labour Research and Resource Centre (LaRRI) (BTI Report, 2018). Religious and civil society organisations and youth movements are often viewed as potential agents of "extremist tendencies" and possible threats to national security within the security establishment (BTI Report, 2018).

3.1 Media landscape in Namibia

Namibia has a very plural (print) media landscape. A variety of independent newspapers are able to report freely and perform as watchdogs. Investigative journalism is an integral part of a few newspapers. In contrast, the Namibia Broadcasting Corporation (NBC) has acted cautiously, refraining from promoting any opinions that are likely to upset the dominant party in political power (BTI Report, 2018). Political officeholders are often non-cooperative when it comes to the independent media, while the minister of Information announced in 2016 plans to regulate the media more closely (BTI Report, 2018). In the same year, the government announced a plan to give preference to state media for advertising, which might be used as a means to increase pressure on privately owned media outlets. For several years, Reporters Without Borders has ranked Namibian among the top 20 countries in the world in terms of media freedom (https://rsf.org/en/namibia). In 2018, the Namibia Central Intelligence Service (NCIS) accused The Patriot (a private newspaper) of endangering "national security" by covering the acquisition of properties by former NCIS members, but the courts ruled in favour of the newspaper. The NCIS case was based on laws dating back to the 1980s and 1990s imposing major restrictions on the dissemination of information concerning national security. Pro-government media are meanwhile getting an ever-larger chunk of the revenue available from advertising, which is threatening the financial prospects of the privately-owned media and independent news coverage (Reporters without Borders, 2019). An independent media ombudsman as well as the Namibia Media Trust are strong advocates for media freedom and critical of state intervention (BTI Report, 2018).

An overview of the Telecommunications Sector in Namibia

In the telecommunications sector, Telecom Namibia, which has offered ADSL access since late 2006, has a de facto monopoly on ADSL access. Their monopoly was unsuccessfully challenged in the courts by Mweb Namibia in May 2007 and again in August 2011. In February 2007, ISP Namibia Mweb began offering broadband wireless services through WiMax, making Namibia the second African country (after Mozambique) to do so. The mobile services sector is dominated by MTC Namibia and TN Mobile, which are wholly owned by the government. It is plausible, therefore, to argue that because of the political economy of the telecommunications sector, the Namibia government might be able to abuse its power position to engage in invasive surveillance of the media and telecommunications ecosystem. There are no government restrictions on access to the internet; however, the Communications Act of 2009 provides that the intelligence services can monitor e-mail and internet usage with authorisation from any magistrate (BTI Report, 2018). There have been some allegations and rumors that the government reviewed ways to block or curtail social media sites, but there is no concrete evidence of such action (Links, 2019). The constitution provides for freedom of speech and of the press, and the government generally respects these rights.

Figure 2: Namibian laws related to privacy

National obligation

6. The Constitution of the Republic of Namibia guarantees the protection and respect of the rights to privacy under Article 13, which states that:

(1) No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.

(2) Searches of the person or the homes of individuals shall only be justified:

(a) where these are authorised by a competent judicial officer;

(b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest, and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied.

International obligations

7. Namibia has ratified the International Covenant on Civil and Political Rights ('ICCPR'), which under Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".

8. The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."4

9. In accordance with Article 144 of the Namibian Constitution "unless otherwise provided by this Constitution or Act of Parliament, the general rules of public international law and international agreements binding upon Namibia under this Constitution shall form part of the law of Namibia."

Source: Privacy International, 2019

However, media reports (Links, 2018) have shown that there are grounds to suspect that there is invasive and unlawful state surveillance in Namibia. In a series of articles published by Frederico Links, titled, 'The rise of the Namibian Surveillance State' which appeared twice in The Namibian newspaper – on Friday 16 February 2018 and Friday 23 February 2018, the author argues that "The formalising of repressive tendencies and security creep should become major concerns on the Namibian political and democratic landscape this year as a number of proposed policy initiatives threaten to undermine a range of constitutionally enshrined human rights." He also reported that the Namibia Central Intelligence Service (NCIS) buying CellXion's IMSI-catcher machine, and the proposed SIM card registration regime – as major areas of concern. The reports also indicated that the security and intelligence elements within the Namibian government have been on a shopping spree for communication interception and surveillance technologies and equipment for most of the last decade, since 2009. Evidence in the articles also suggest that the Namibian government has procured communication interception and surveillance technologies and equipment from firms based in the European Union (EU) and the United Kingdom (UK).

However, Charles Siyauya, the Ministry of Information and Communication Technology, responded to Links in an article titled Namibian surveillance state: A response to Frederico Links (published in the New Era on 2 March 2018), arguing that, "to spy on citizen/s is the least on the priority list of execution of any progressive government. Only a predatory or failed government can spy on its citizens. Intelligence must be understood as a vital instrument of the state and a profession, which satisfies a patriotic desire. Intelligence is about protecting the country and citizens from external and internal threats; it is about economic security, environmental security, social security, protecting visitors, properties and natural resources, etc. Frederico Links ought to focus on a broader picture of intelligence than limiting himself on spying. Although intelligence is secret by nature, a better understanding, application and relevance of intelligence in democracy and national development must be shared".

Episodic media reports have played an important role in exposing cases of communication surveillance and the abuse of public funds by the NCIS. For instance, Shinovene Immanuel, a former reporter with The Namibian broke a story titled, "Spy agency gets N$217m…over 3 years[6]". Some of these public funds are believed to have been used to buy surveillance technologies. However, in the national budget these expenditure items are often hidden under headings like construction, renovations and improvements.

The media have won court cases against NCIS. For instance, the NCIS tried to block a local newspaper, The Patriot in 2018, from reporting how former members of the spy agency were using farms bought for N$58 million for private use.

6 https://www.namibian.com.na/187215/archive-read/Spy-agency-gets-N$217-million-over-3-years

4. Methodological Approach

This study was anchored in qualitative research methodology. This methodology is used to answer questions about experience, meaning and perspective, most often from the standpoint of the participant (Hammarberg, Kirkman and de Lacey, 2016). Qualitative research techniques include 'small-group discussions' for investigating beliefs, attitudes and concepts of normative behaviour; 'semi-structured interviews', to seek views on a focused topic or, with key informants, for background information or an institutional perspective; 'in-depth interviews' to understand a condition, experience, or event from a personal perspective; and 'analysis of texts and documents', such as government reports, media articles, websites or diaries, to learn about distributed or private knowledge (Hammarberg et al., 2016).

For the purposes of this mapping exercise, the author relied on a combination of qualitative policy analysis, document analysis and in-depth interviews with key informants. Qualitative policy analysis was used to make sense of existing policies, bills and policy briefs from the Ministry of Information and Communication Technology and other non-state actors such as the Namibia Media Trust (NMT) and Institute of Public Policy Research (IPPR). The author also used document analysis to tease out the policy discourses emerging from shadow reports and press statements by the Namibia Media Trust (NMT) and Institute of Public Policy Research (IPPR). 13 in-depth interviews were conducted with key informants drawn from Windhoek City Police, journalism (journalists who have covered the issue of communication surveillance), officials from the regulatory body (CRAN), mobile service providers (MTC), media advocacy organisations (NMT and Namibia Action Group), officials from the Ministry of Information and Communication Technology and NCIS. Informed consent was sought and anonymity was guaranteed due to the sensitive nature of the research.

5. Preliminary Findings

The first section (see 5.1) addresses findings culled from qualitative policy analysis and document analysis while the second section (5.2, 5.3 and 5.4) focuses on data sourced through key informant interviews conducted in Namibia.

5.1 The basis of state surveillance concerns in Namibia

Besides media reports (see Links, 2018) and policy briefs (Privacy International, 2017), in 2016 the UN Human Rights Committee[7] notably urged the government of Namibia to reform the surveillance framework and strengthen privacy protections. In the 2016 UPR WG report that raised concerns around the issues of surveillance powers and the right to privacy, including mass surveillance, retention of communication data, judicial authorisation, transparency, oversight, and regulating intelligence sharing, the Committee urged Namibia to come out clean on the operations of interception centres.

The UPR WG report (2016) states that: "The State party should ensure that the interception of telecommunications may only be justified under limited circumstances authorised by law with the necessary procedural and judicial safeguards against abuse, and supervised by the courts when in full conformity with the Covenant." The report also raised concerns that surveillance shrouded in illegality was already in motion thereby violating constitutionally enshrined human rights, specifically freedom of expression and the right to privacy, among others. Although the UNHRC[8] requested the Namibian government to respond to surveillance concerns, nothing has so far materialised and no measures have been taken to address these recommendations.

5.1.1 Part 6 of the Communications Act of 2009

Part 6 of the Communications Act 8 of 2009 regulates communication surveillance by the government. The government, though, claims that Part 6, comprising sections 70-77, is not yet in force after a decade and will only come into force on a date set by the Minister by notice in the Government Gazette. Hence, they're arguing that this means they don't have to comply with it. Interviews conducted by the author revealed that there is strong belief amongst opposition parties and civil society actors in Namibia that the Act is already in operation behind the scenes. Below is an except from the Communications Act:

7 https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNAM%2fQ%2f2&Lang=en

8 https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNAM%2fQ%2f2%2fAdd.1&Lang=en

Figure 3: Part of the Communications Act of 2009

Interception centres

70. (1) The President must establish such interception centres as are necessary for the combating of crime and national security.

(2) Interception centres are staffed by such staff members in the Namibia Central Intelligence Service as may be designated by the Director-General with the approval of the Security Commission established by Article 114(1) of the Namibian Constitution.

...continued

(3) Before a staff member performs any function with relation to interception or monitoring of telecommunications contemplated in this Part, he or she must before the Judge- President in chambers make an oath in the following form:
'I, A.B, do hereby swear and solemnly and sincerely promise that I will to the best of my ability perform all functions relating to the interception of telecommunications in accordance with the law of Namibia and that I will not knowingly participate in or assist with any interception or monitoring of telecommunications that is not authorised by the law of Namibia.

(4) A staff member designated in terms of subsection (2) may, in lieu of an oath, make a solemn affirmation in corresponding form.

(5) Interception centres must be equipped by such equipment and software as may be designated by the Director-General.

(6) Interception centres must be funded from such moneys appropriated by Parliament and paid into the account referred to in section 10 of the Namibia Central Intelligence Service Act, 1997 (Act No. 10 of 1997).

(7) The Director-General must designate a staff member in the Namibia Central Intelligence Service as the head of every interception centre.

(8) Where any law authorises any person or institution to intercept or monitor electronic communications or to perform similar activities, that person or institution may forward a request together with any warrant that may be required under the law in question to the head of an interception centre.

(9) Any staff member employed in an interception centre may do anything necessary in order to perform the interception or monitoring concerned (as well as any decoding or decryption necessary to make the information in question intelligible) and must forward all information obtained from these activities to the person who made the request referred to in subsection (8).

(10) Any provision in any law requiring a person to provide assistance with interception or that authorises the issue of a warrant or other order compelling or requiring a person to render assistance with interception is construed so that the assistance in question includes the provision of a key or other information necessary to make any information obtained by the interception in question, intelligible.

(11) The Director-General may issue directives in which he or she determines -

1. **(a)** how information obtained by interception must be handled;
2. **(b)** which persons may handle information obtained by means of interception;
3. **(c)** which persons may perform any action relating to interception;
   (d) any other technical or procedural matter relating to interception that is necessary or expedient in order to ensure that information obtained by means of interception is only used for its intended purpose and that the objects of this Part are fulfilled.

(6) The tariffs prescribed in terms of subsection (1)(b) -

1. **(a)** may differ in respect of different categories of telecommunication service providers; and
2. **(b)** must be uniform in respect of each telecommunication service provider falling within the same category.

(7) The compensation prescribed in terms of subsection (1)(b) may only be for direct costs incurred in respect of personnel and administration which are required for purposes of providing any of the forms of assistance contemplated in subsection (1)(a).

Source: Republic of Namibia Communications Act 8 of 2009

It can be deduced from the above that the Communication Act, Act No.8 of 2009 provides for the interception of telecommunications in Namibia. Part 6 provides for the establishment of interception centers, which are defined as necessary for the combating of crime and national security. Interception centres are staffed by staff members in the Namibia Central Intelligence Service (NCIS) as may be designated by the Director-General with the approval of the Security Commission established by Article 114 (1) of the Namibian Constitution (Communication Act, 2009). The Communication Act stipulates that before a staff member (NCIS) performs any function in relation to interception or monitoring of telecommunications contemplated in Part 6, he or she must be present before the Judge-President in chambers and make an oath and obtain consent of a judge. The Act makes provision for penalties and offences for contravention of the provisions of the Act.

5.1.2 Role of Chinese telecommunication giants especially ZTE and Huawei Technologies in the Namibian telecommunications sector

Over the past 12 years, there has been a significant involvement of Chinese firms Huawei Technologies and ZTE on the continent in general and in the Namibian telecommunications sector in particular (Links, 2018). In several African countries, Chinese technology infrastructure serves as the backbone of network infrastructure (Xinhua, 2018). Namibia has not been left out of this trend of awarding infrastructural development projects to Chinese companies. As pointed earlier, these Chinese telecommunication companies have over the years been reported to enable spying by the Chinese state. There are allegations that devices running on Chinese-made systems could provide a backdoor for Beijing to spy (Dahir, 2018).

On the one hand, Huawei, which is arguably one of the world's leading purveyors of surveillance technology, has a big footprint in Namibia and was responsible for overhauling Telecom Namibia's operating system over the last decade (Xinhua, 2018). The Chinese company Huawei and MTC have been in a technological transfer partnership with the Namibian Government-owned MTC for the past twelve years. Huawei has provided services like SingleRAN solution, and the DWDM 40G fiber transmission to MTC Namibia. In partnership with MTC and Telecom Namibia, Huawei is estimated to be serving 2 million Namibians with voice communication, internet access and digital television programmes using hundreds of radio base stations and thousands of kilometres fiber connectivity all over the country. The company has also secured supply and technological support service contracts with the Namibian fixed-line operator, Telecom Namibia, and mobile network operator MTC (Links, 2019). Huawei has also partnered with the public broadcaster, the Namibian Broadcasting Corporation (NBC), on the Digital Terrestrial Television project (Links, 2019).

The involvement of Huawei Technologies in the Digital Terrestrial Television[9] project also raises very pertinent questions. It is not clear whether the project gave the Chinese giant tech company access to back-end infrastructure, which can be used by the government of Namibia for surveillance purposes. As part of digitalisation, there are fears amongst civil society organisations that smart technologies can be used for other purposes beyond the installation of radio and television signals. This was revealed through interviews with members of civil society organisations in Windhoek, Namibia.

On the other hand, ZTE products, such as phones and internet routers, are also easily purchasable in Namibia (Links, 2018). In view of the foregoing, it is reasonable to suppose that these

9 This is concerned with replacing analogue terrestrial television broadcasting with digital terrestrial television (DTT) broadcasting. DTT enables broadcasters to transmit at lower power than in analogue transmission, without reducing the coverage area, and whilst simultaneously improving the quality of the consumer's viewing experience.

firms, given their associations with Namibian state-owned telecoms companies, would also be drawn, upon request, into helping make the mobile service environment interception and surveillance-friendly for state security agencies.

5.1.3 Acquisition of surveillance technologies

Reports suggest that Namibia is one of the countries that had purchased interception and surveillance technologies from several companies across the globe (Motherboard Magazine, 2016; Links, 2019). For instance, in 2016, Motherboard magazine was able to get the information of companies selling such technologies and countries buying the equipment through a freedom of information request to Britain's department for international trade. It is believed that Namibia was able to buy surveillance technologies such as IMSI-catchers[10]. The IMSI-catchers are devices that act like fake cell towers, which trick a target's device to connect to them and then relay the communication to an actual cell tower of the network carrier. This way all of the target's communications – calls, text messages, Internet traffic, etc. – go through the IMSI-catcher and can be collected and read or listened on. With the help of a SIM, it simultaneously logs into the GSM network as a mobile station. The IMSI-catcher can induce the mobile station to use no encryption at all. Hence it can encrypt the plain text traffic from the mobile station and pass it to the base station.

Anecdotal evidence (Links, 2018) suggests that these tools were bought by the Namibian government and are being used by the security services to intercept cellphone signals. The British company from which Namibia appears to have bought IMSI-catchers (Motherboard Magazine, 2016), is CellXion Ltd, which is based in Caterham, Surrey, and offers "cellular intelligence solutions". In the dataset released by the British department for international trade it states that three export licences were issued for "telecommunications interception equipment" to Namibia, of which one was for a "Searchlight UMTS/GSM detection and location system", which is an IMSI-catcher.

RADWIN, the global broadband wireless leader, announced that the Windhoek Police Department in Namibia built a state-of-the-art wireless video surveillance network leveraging RADWIN's wireless broadband access solutions (RADWIN, 2016). RADWIN's Point-to-Multipoint was installed in dozens of crime hot-spots throughout the city. The systems transmit high-quality video from the cameras directly to police headquarters, enabling on-the-spot detection and response to events (RADWIN, 2016). RADWIN's Point-to-Multipoint systems, which deliver dedicated bandwidth per camera site with 90% uplink traffic and mega-capacity of up to 750 Mbps, as well as RADWIN's Point-to-Point systems for backhaul (RADWIN, 2016).

Whilst there has been no official presented by the government on the use of these acquired, it seems reasonable to assume that since making the purchase sometime between February 2015 and April 2016, that Namibian security authorities have deployed the equipment, and might actually have purchased more such technologies in 2017 (Links, 2018). This raises an issue of legality, as Namibian authorities officially continue to maintain that Part 6, which authorises telecommunications interception of the Communications Act of 2009 has not been published in the official government gazette and operationalised.

5.1.4 Government monopoly in the telecommunications sector

The government of Namibia holds almost 90 percent stake in the telecommunications sector. This ownership structure provides the government total control over the operations of fixed and mobile service providers. There are also concerns this would enable the government to use its major shareholder status to push for installation of surveillance technologies in the country's telecommunication ecosystem.

10 It is a device, which can monitor large numbers of mobile phones over broad areas.

This monopoly can also allow the government to direct telecommunication service providers to undertake Internet or even social media shutdowns, as has been reported in other African countries.

For instance, Mobile Telecommunications Limited Namibia (MTC-Namibia), a mobile phone company 66% of which is owned by Namibia Post and Telecommunications Holdings (NPTH) and Telecom Holdings Limited which is intern wholly owned by the Namibian Government (the rest of the shares are owned by Portugal Telecom.) The company currently covers 95% of the country's population of nearly 2.1 million with a dual band 900/1800MHz GSM network, plus a 3G HSDPA+ network, making for a download speed of up 21.6Mbps in Namibia's major towns, as well as LTE services (up to 100Mbps).

TN Mobile is a mobile telecommunications company 100% owned by Telecom Namibia, which is owned by Namibia Post and Telecom Holdings Limited, which is intern wholly owned by the Namibian Government. Telecom Namibia, is a commercialised subsidiary of Namibia Post and Telecom Holdings Limited, which is intern wholly-owned by the Namibian Government.

This powerful position arguably puts the government of Namibia in a place where it's able to use its "ownership muscle" to engage in invasive and pervasive surveillance. Furthermore, PowerCom (Pty) Ltd is another government-owned parastatal heavily involved in the construction, acquisition, maintenance, leasing and management of tower space (PowerCom Website, 2019). The company is a 100% subsidiary of Telecom Namibia. As a tower infrastructure provider, PowerCom has 300 telecommunications towers across the country and over 20 rooftops under its management. The firm's infrastructure enables television and radio broadcasters throughout the country by leasing tower space to them. Security companies also rely on PowerCom's infrastructure for increased connectivity in their sector. This allows the government through the security services to install surveillance technologies on towers, which are built, leased and managed by PowerCom. Because of its majority shareholder status over all the fixed and mobile service providers, the government of Namibia would, in theory, be able to exercise total control over the country's internet gateway systems.

5.1.5 Lack of regulatory independence on the part of CRAN

Besides ownership issues discussed above, there are also deep-seated regulatory concerns. The acquisition of surveillance technologies in an environment where the country's converged media regulator (the Communications Regulatory Authority of Namibia, or CRAN) does not seem to be fully independent casts doubt about its ability to push back against unconstitutional surveillance practices.

CRAN regulates telecommunication services and networks, broadcasting services, postal services and the use and allocation of radio spectrum in Namibia. The regulator is mandated by Communications Act (No. 8 of 2009) to grant, renew, amend, transfer, suspend and revoke licenses in the areas of broadcasting and telecommunications service in Namibia.

Partly because the board of directors are appointed by the president and partly because CRAN governance falls within the Ministry of Information and Communication Technology, CSOs have begun to question the regulatory independence of the organisation. There are concerns amongst media advocacy groups that CRAN is a captured entity with little space to manoeuvre especially at the hands of powerful political actors. One notable example dates back to 2017, when the then Minister of Information and Communication Technology was accused of putting undue pressure on CRAN to launch a single internet gateway system.

5.1.6 The push by the government for the roll-out of the Single Internet Gateway system

In 2017, the government, through the Minister of Information, communication and Technology,

Mr Tjekero Tweya attempted to push through an idea of launching a Single Telecoms Gateway (also known as Single Internet Gateway, SIG) in Namibia (Links, 2018).

A Single Internet/Telecoms Gateway has the potential to force all voice/data communication in Namibia through a single gateway effectively making it a choke point and stifle competitiveness, since one company will be mandated to set the price of how voice/data communication are sent into and out of Namibia. The company that would set up the SIG would become the de-facto telecom monopoly in Namibia as all current telecoms will have to pay for and use its gateway for access to the outside world (Emvula, 2017).

The move was criticised by media advocacy organisations for being ultra vires the constitution and in conflict with the Communications Act. The Namibia Media Trust[11] (2017) argued that a single gateway would serve the main purpose of enabling surveillance and monitoring of communication of citizens, and in the wrong hands, could lead to potentially draconian moves such as internet shutdowns: this in turn would rob Namibians of their rights to free expression and access to information and communication. Therefore, the NMT[12] (2017) urged the government of Namibia to abandon this single telecoms gateway proposal in its entirety, as it will entail higher costs for consumers and enables undue surveillance.

5.1.7 Concerns of surveillance of Members of Parliament

The issue of the donation of 157 Huawei MediaPad M3 Lite tablets to Members of Parliament (MPs) to the tune of N.dollars 700,000, through the Ministry of Information and Communication Technology (MICT) also created a major talking point around corporate-enabled surveillance. These concerns were raised by Members of Parliament from the opposition and ruling parties who feared that they could fall prey to the surveillance machinations of the donor. The Popular Democratic Movement (PDM) rejected the gifts, saying that the company has business interests in Namibia and wants to bribe politicians in winning certain contracts[13]. Other MPs from the opposition and the ruling parties demanded assurance from the MICT that the devices are safe from espionage, following global reports that Huawei was spying for the Chinese government[14]. The questions stem from international reports (Dahir, 2018) that the Chinese government is using Huawei's tech devices, such as mobile phones and tablets to spy on politicians and prominent people in foreign countries. The MICT responded to the concerns by explaining that the ministry did not blindly accept the gifts from Huawei Technologies[15]. They took into consideration relevant security issues associated with the brand.

5.1.8 The existence of interception centres

Interviews with key informants in Namibia indicated that Part 6 of the Communications Act of 2009 was still to be implemented. The provisions of the same Act outlines that "licensees and other providers of telecommunications services must provide a telecommunications service in such a manner that it is capable of being intercepted". The Act also notes that licensees and other providers of telecommunications services must store such information relating to the originator, destination, contents of, and other information relating to the telecommunications concerned as may be prescribed. This suggests mobile and fixed service telecommunication operators will serve as choke points through which communication surveillance takes place in Namibia, thus, compelling service

11 https://www.namibian.com.na/168049/archive-read/Namibia-Media-Trust-slams-Tweyas-deal
12 https://economist.com.na/27273/speak-your-mind/far-reaching-implications-for-a-single-telecoms-gateway-for-internet-access/
13 https://www.lelamobile.com/content/75611/PDM-rejects-Huawei-tablets/
14 https://www.namibiansun.com/news/mps-wary-of-chinese-gifts2018-06-21
15 https://www.namibiansun.com/news/mps-wary-of-chinese-gifts2018-06-21

providers to build into their systems surveillance and monitoring capabilities threatens the integrity, security and privacy of communication systems (Privacy International, 2017). This is even more serious especially in a country where the government is the majority shareholder of all the fixed and mobile service providers (such as Telecom, MTC and TN Mobile). Telecommunication service providers are expected to acquire at their own cost, either by purchasing or leasing, the facilities and capabilities necessary to engage in communication surveillance.

Authoritarian-inclined policy and regulatory proposals began to take shape between 2017 and 2018, thereby heightening the belief that surveillance might have been normalised and institutionalised in post-apartheid Namibia (Links, 2019).

Figure 4: Namibian laws enabling communication interception and surveillance

There are a number of laws on the Namibian statute books that enable or have a significant bearing on communication interception and surveillance in some form or other, whether as part of evidence gathering in criminal matters or telecommunications interception for anti-terrorism purposes.

These laws are:

- Criminal Procedure Act of 197734
- Protection of Information Act of 1982
- Police Act of 1990
- Namibia Central Intelligence Service Act of 1997
- Communications Act of 2009
- Financial Intelligence Act of 2012
- Prevention and Combating of Terrorist and Proliferation Activities Act of 2014

Source: Frederico Links (2019), Spying on Speech, Democracy Report, Special Briefing, IPPR.

Building on the Communications Act of 2009, the proposed Electronic Transactions and Cybercrime Bill of 2017[16] permits for the creation of interception centres in the interests of combating crime and national security. The objects of the Act are – (a) to provide for the development, promotion and facilitation of electronic trans- actions and related communications; (b) to remove and prevent barriers to electronic transactions and related communications; (c) to promote legal certainty and confidence in electronic transactions and communications; (d) to promote e-government services and electronic commerce and communications with public and private bodies, institutions and citizens; (e) to develop a safe, secure and effective environment for the consumer, business and public agencies or bodies to conduct and use electronic transactions; (f) to promote the development of electronic transaction services responsive to the needs of online consumers; (g) to ensure that, in relation to the provision of electronic transactions and services, the special needs of vulnerable groups and communities and persons with disabilities are duly taken into account; (h) to ensure compliance with accepted international technical standards in the provision and development of electronic transactions and related communications; and (i) to ensure that the interest and image of Namibia are not compromised through the use of electronic transactions and communications.

16 http://www.mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25

Like in other jurisdictions, the definition of national security is not clear and at most very vague and broad. This can easily be abused to justify intrusive surveillance of individuals in the name of 'national security'. As it currently reads the Bill would permit full access to personal data and any online communication of individuals. State security could, thus, access or tap into personal information and communications, without being subject to much or any scrutiny. An analysis of the Bill shows that there are a number of problematic aspects such as secret warrants and warrantless search and seizures; lack of data and privacy protection; undermining of encryption and anonymity; as well as excessive and unaccountable ministerial power. There is need for the government of Namibia to adhere to national and international obligations in order to protect rights and freedoms of its citizens.

5.1.9 Absence of judicial authorisation and transparent oversight mechanisms over the intelligence agencies

The existing and proposed legislation do not adequately address the issue of strong and transparent oversight mechanisms[17]. There is no judicial authorisation granted to the Director General of Namibia Central Intelligence Service (NCIS) and therefore, it is unclear how accountability and transparency are built into the surveillance architecture. The intelligence organisation operates from the office of the President and there is little information in the public domain about its operations.

The intelligence service is regulated by the Namibian Central Intelligence Service (NCIS) Act, 1997 (Act No 19, 25. 1997). The Act sets out clear safeguards to prevent abuse and upholds Article 13 of Constitution of the Republic of Namibia and guarantees the protection and respect of the rights to privacy. The 1997 Act provides a strict legal framework for the NCIS to conduct targeted interceptions of communication over telecommunications networks, which under Article 25 requires it to obtain a High Court warrant, which rests on the presentation of evidence of a serious threat to national security, and it prevents it from conducting fishing expeditions, as the request must be specific to a type of communication and target. It's not clear however how metadata and intrusive powers of the intelligence services are regulated in the current legislation.

The Communications Act of 2009, includes little or no safeguards to protect the right to privacy and the confidentiality of users' data, metadata and information, expanded the powers of the intelligence agency to conduct surveillance without judicial authorisation. In essence, this overtook the NCIS Act of 1997's provision. The only provision which seems to include some protection is Article 121 (3), which says that the power awarded to the Authority to monitor compliance with the provisions of this Act, do not allow the Authority to use the Act "to obtain the contents of any message or information transmitted over that network, or to obtain any information relating to the behaviour of any customer or user of any telecommunications service".

There are no attempts to include the necessary and proportionate principles[18] in the current and proposed laws. The laws do not provide oversight safeguards against the risk of abuse of such systems, and are substantially weak or almost completely silent on personal privacy and data protection measures. It is urgent to implement a more democratic, transparent and accountable oversight mechanism. The independence of the judiciary and the media regulator (CRAN) has been questioned in recent years by civil society organisations in Namibia (see African Media Barometer-Namibia, 2018).

17 https://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global

18 https://necessaryandproportionate.org/principles

5.1.10 The proposed Electronic Transactions and Cybercrime Bill

Another controversial piece of legislation relates to the proposed Electronic Transactions and Cybercrime (ETC) Bill[19] of 2017. Although it has been shelved for a number of years, the Bill in its current form will allow the government of Namibia to conduct search and seizure operations of databases and computers, the interception of data and communication, as well as remote monitoring for a period of up to three months. It also forces telecommunications service providers, or any other entity that may have information relating to a matter of interest to the government, to co-operate and provide all relevant data.

These proposals would empower law enforcement and security agencies to engage in widespread communication interception and surveillance (with indications being that they are already quite extensively engaging in such activities), with the cooperation of telecommunications and internet service providers, while affording the public very little data and privacy safeguards and not providing for meaningful oversight mechanisms to prevent interception overreach or surveillance abuse (Links, 2018). The introduction of the ETC Bill has been characterised as a "legal cover" to justify the already happening practice of state surveillance (Links, 2019).

Fortunately, the Bill was swiftly withdrawn again from the parliamentary agenda following an outcry from sections of civil society (Namibia Media Trust, 2018). Amongst what civil society actors were flagging and objecting to were sections of the bill which appeared to enable warrantless communication interception and surveillance, as well as not providing for proper interception and surveillance oversight mechanisms and some level of transparent accounting for such practices. This shows evidence of effective activism around surveillance and intrusive monitoring in Namibia.

19 http://www.mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25

5.1.11 Calls for mandatory SIM-card registration

In 2017, the NCIS (at a two-day closed-door "national multi-stakeholder" workshop, on "preventing and countering violent extremism") and the Ministry of Information and Communication Technology made a proposal that there was "a need to urgently implement the requirement for telecommunication service providers to register SIM cards against the name of owners" and "a need to devise mechanisms to monitor social media with the aim to detect extremist tendencies" (Links, 2018). Even mobile service providers in Namibia have supported this idea arguing that it was critical for ensuring the safety of cellphone users and the security of networks. The proposal was also buttressed during the November 2017 SWAPO Congress. The ruling party congress ultimately resolved that a Ministry of Cyber Security be established in order to control information in the social media and guard against cyber-crimes such as hacking and monitor illicit financial flows.

The clarion call for the introduction of a formal SIM card registration regime fronted by NCIS was aimed at dealing with "extremist tendencies". This is despite an array of evidence (GSMA, 2016; Gow and Parisi, 2008), which shows that there is no correlation between SIM card registration and effective crime prevention. SIM card registration allows the state to know the identity of the owner of a SIM card, and thus who is most likely making a call or sending a message (Privacy International, 2018).

Mandatory SIM card registration eradicates the potential for anonymity of communication, enables location-tracking, and simplifies communication surveillance and interception. It can also be used in conjunction with an IMSI catcher to know the possible identities of everyone in a particular area (Privacy International, 2018). By facilitating the creation of an extensive database of user information, it places individuals at risk of being tracked or targeted, and having their private information misused (Privacy International, 2018).

In the absence of comprehensive data protection legislation and judicial oversight, SIM users' information can be shared and matched with other private and public databases, enabling the state to create comprehensive profiles of individual citizens (Privacy International, 2018).

Notwithstanding, this evidence (Gow and Parisi, 2008; GSMA, 2016) that the crime and terror fighting effectiveness of SIM card registration regimes appears to be wildly over-hyped, many governments, notably African governments and their internal technical supporters (such as state-owned telecoms operators), have pushed ahead with implementing such systems (Links, 2018).

Research in South Africa has shown that spying – targeting journalists, civil society activists and political opposition – is pervasive and intrusive (see Duncan, 2018; Mare, 2016). In South Africa, the government of President Cyril Ramaphosa has since appointed a high-level review panel to assess the State Security Agency's mandate. Its mandate was to ensure that the country reconstruct what is a responsible and accountable State Security Agency, which works in line with relevant legislation and the Constitution.

5.1.12 Lack of a comprehensive data protection law

It is important to note that Namibia does not have a comprehensive data protection law. During a media stakeholders workshop held in April 2019, the Minister of Information and Communication Technology, Mr Stanley Simaata, revealed that a data protection bill will be brought before the Namibian parliament sometime in 2019. An analysis of the proposed bill conducted by the researcher shows that it would include the establishment of Data Protection Authority (DPA) under Section 3 to 12, as well as ten principles of data protection including accuracy (Sec. 13) legitimacy (Sec. 15), purpose (Sec. 15), necessity and proportionality (s 14), fairness (s 14), security and confidentiality (sec. 26), transparency, and stringent protection for sensitive personal data and personal data used for marketing. This is in many respects considered a very low standard since magistrates typically don't have specialised knowledge on data protection.

The proposed Data Protection Authority of Namibia oversees the implementation of the law. However, the data processors and controllers must be subject to rigorous regulations providing them with standards on how to handle any data they process; be compelled to be transparent and accountable; be subject to checks and balances; fulfill the rights of individuals and respect the rule of law.

The data protection legislation must be accompanied by effective implementation and enforcement (Privacy International, 2018). This requires that an independent regulator or authority must be appointed to ensure the protection law is enforced, and it must have the mandate and resources to conduct investigations, act on complaints and impose fines when they discover an organisation has broken the law. It is also important to have a strong and critical civil society as a watchdog, with the ability to raise complaints, research abuses and be constantly vigilant of implementation.

5.2 Primary data from key informant interviews

5.2.1 Surveillance capabilities in Namibia

The study attempted to find out the capabilities of surveillance technologies in Namibia. Despite efforts to obtain primary information, interviews with various stakeholders in the national intelligence and police services failed to fully unpack the capabilities of the surveillance technologies.

There was a general sense of fear amongst the interviewees that the covert operations information was too sensitive for it to be made public. Thus, whilst the technological surveillance capabilities of Namibia remains largely unconfirmed by official resources, the fact that the country has acquired IMSI catchers, sophisticated surveillance video

cameras and other related gizmos raises serious concern with regards to how these technologies are being deployed, bearing in mind that part 6 of the Communication Act of 2009 is technically still not yet in operation.

However, interviewees from the Windhoek City Police indicated that the capital had installed a total of 93 high-resolution surveillance cameras across the city for the purposes of fighting crime. Respondents from the security services refused to comment on whether the surveillance cameras are sometimes used for mass and targeted surveillance of ordinary Namibians. Security officials who were interviewed for the research, however, stated that these CCTV cameras, which are of different types, have been placed in hotspots around the city (especially areas where breaking of the law has been prevalent.)

Without giving away the types of cameras used as sensitive security information, they indicated that the prices of the cameras range between N$20,000 (USD 1200) and N$60,000 (USD 4000), giving an indication that these cameras are not ordinary cameras but advanced smart surveillance technologies. The police also refused to comment regarding the place where these cameras were bought and how they source for training for their usage. But they admitted that these CCTV cameras are not only installed in the Central Business District but also in residential areas, thereby giving an indication of the real possibility to use the cameras for surveillance activities other than crime fighting. Below is an extract from one of the interviews:

"Since the installation of cameras around Windhoek, the crime trend in those areas has drastically gone down especially theft of motor vehicles in the central business district (CBD). The same with neighbourhood areas where cameras are installed, there's an improvement"

(Respondent, Security Services in Namibia).

In view of the capacity and the extent to which the security forces are capacitated to carry out mass surveillance if the need arises, interviewees observed that the police was financially constrained and without adequate funding to install more surveillance cameras in Windhoek at the moment.

Worryingly, there is no CCTV policy or framework in Namibia and, thus, conducting surveillance using these technologies in a policy vacuum context can easily be abused by rogue elements. Interviews with CSOs indicated that there were no consultations in the roll-out of CCTV cameras besides justifying them as crime fighting technologies.

In terms of the procedure, which is followed when the State or any other third party requires having access to the footage from the surveillance cameras, the security services had this to say:

"If an incident is monitored and the footage is needed, there are forms to be completed and the footage will be retrieved. This is currently only done when and if the footage is needed for court proceedings. This has been used a lot of times where CCTV footage obtained from the City Police was used to apprehend suspects"

(Respondent, Security Services in Namibia).

Interviewees explained that surveillance technologies were primarily used for crime fighting purposes in Namibia. They also refused to shed light on whether there are cases where these cameras are often used for targeted or mass surveillance. These concerns were generally raised by journalists and members of CSOs.

An official from one of the mobile service providers declined to answer the question on whether his company was involved in communication surveillance. Instead, he offered a very short response in view of the assumed role of mobile and fixed telecommunication operators as choke points in Namibia. He said the following:

"Ours is an entity that protects the privacy of its customers and will not reveal customers data to any third party including the State, unless only when the data is requested formally in a letter from the High Court justifying also that it is in the best public interest to avail such data. Otherwise, we never share our customers' data with anyone."

The above interview extract highlights the fact that there are cases where third parties requested information from mobile service providers in Namibia. Although this claim was not supported by any transparency report from the main mobile service providers, it is plausible to speculate that this highly likely given the secretive nature of the operations of interception centres. Given that the government of Namibia is a major shareholder of all the telecommunications companies in the country, it is not far-fetched to speculate that it can abuse its ownership muscle to request for customers' data without going through the High Court route.

Interviewees from civil society organisations observed that there were opaque deals between Chinese telecommunications giant Huawei Technologies and several African countries, including Namibia[20]. They suggested that the roll-out of facial recognition technology in Zimbabwe was simply a launchpad for other countries in the Southern African Development Community (SADC) region to follow suit. There is very little information available about Namibia's engagements and dealings with Chinese vendors of communication interception and surveillance technologies and equipment (Links, 2018).

Respondents from civil society raised concerns with the role played by Huawei and ZTE in the implementation of the country's network infrastructure. They had this to say:

"As Namibians, we are concerned about the involvement of Chinese companies in our telecommunications sector. Companies like Huawei had a bad international record. They have been implicated in the spying of the AU headquarters and currently their 5G technology has been criticized for aiding surveillance on behalf of the Chinese government"

(Member of civil society organisation)

"The hackability of Huawei technologies is a major concern. We are not sure if they do poor coding of their systems to aid surveillance or it's simply a case of poor workmanship. In Namibia, we understand Huawei has been granted lucrative contracts by all the major telecommunication operators. This somehow means they have access to our national key point infrastructure. Given the non-interference stance of China, it's very possible that Huawei can cooperate with certain political elements to install surveillance technologies on our network infrastructure"

(member of civil society organisation).

Overall, it is not clear whether the cozy relationship between Chinese tech giants and telecommunication operators in Namibia has translated to the level of purchase and installation of surveillance technologies.

5.3 Who are the targets of communication surveillance in Namibia?

Information discussed in this section was gathered from key informant interviews with participants from civil society organisations, police, regulatory authorities and journalists.

Interviews with various key informants in Namibia revealed that they believe that the main targets of communication surveillance included investigative journalists, members of the civil society organisations, political factions within the ruling party and some opposition politicians[21]. The idea that surveillance technologies were being used to spy on political factions within SWAPO was revealed in March 2014, when a ruling party member, Kazenambo Kazenambo accused the

20 https://www.lelamobile.com/content/75611/PDM-rejects-Huawei-tablets/

21 https://ippr.org.na/wp-content/uploads/2019/06/IPPR-surveilance-web.pdf

government of abusing its power to conduct lawful interception (Links, 2019). The situation was more pronounced during the run-up to the last presidential elections where Team SWAPO and Team Harambee engaged in highly publicised[22] mudslinging contests on traditional and social media platforms.

Members from the civil society organisations who were interviewed were very wary about the possibility of communication surveillance compromising their privacy and confidential communication[23]. Some of them expressed a huge concern with the institutionalisation of communication surveillance:

"We know it for a fact that there has been infiltration of civil society organisations in the last few years. Indeed, telecommunication surveillance is happening in Namibia. The soft targets are mainly factions within SWAPO, journalists, members of the civil society organisations and communities, which have harboured secessionist intentions, for instance those in the Caprivi region"

(Member of civil society organisation).

"The issue of surveillance of private citizens is something that has occupied us and is being discussed by various stakeholders because it's a part of the new cyber-security laws that are set to come into force when approved by Parliament"

(Member of civil society organisation).

Confidential interviews with selected journalists indicated that the practice of surveillance was being used to intimidate investigative journalists in the newsrooms. Some of the quotes below help to contextualise these claims of perceived or experienced surveillance:

"Our phones and emails are bugged, we know that. In some cases, our emails take more than a day to be delivered. These are signs that our communication is being routed through some kind of interception centres"

(personal communication with a former journalist).

"We know there are spies in the newsrooms who serve as informants for NCIS. These people are known. I know in one newsroom people talk about it openly. And the culprits are known"

(Journalist).

Others spoke about surveillance as a huge possibility in Namibia with some of the activities of State organs such as the NCIS giving some indication that there could be surveillance. This is partly attributable to evidence published by Motherboard Magazine, which showed that Namibia has been buying surveillance technologies from European vendors. Here is what some of the interviewed journalists had to say:

"Not to my knowledge have I heard of a journalist being placed under surveillance. However, that does not mean to say that it has not happened in the past or present. Efforts by government to at one stage toy with the idea of the Spy bill (ETC, as mentioned earlier) gives one reason to be alarmed that authorities would like to monitor its citizens, in particular journalists. In that instance, I would say they were testing the waters to see what kind of reactions come out from stakeholders had it to be legalised"

(Investigative journalist).

"The activities of the NCIS are of a secretive nature that one does not know the extent of their surveillance capabilities. I do believe that there is, however, a certain degree of competence. The prospects of surveillance always rise when the state is on the back foot and the current state of the economy may compel government to get intelligence on what citizens are thinking and or planning"

(Journalist).

22 https://neweralive.na/posts/shaningwa-tired-of-teams-harambee-and-swapo

23 https://ippr.org.na/wp-content/uploads/2019/06/IPPR-surveilance-web.pdf

"Surveillance of journalists will not bode well for Namibia's media ranking (currently ranked number 1 in Africa by the Journalists Without Borders in terms of media freedom) and all efforts need to be made to ensure the smooth operation of the Fourth Estate, the media. The media as an instrument of development needs to be protected and this is achievable through law that protect data"

(Journalist).

With regards to the last quote, various CSOs and media advocacy organisations[24] called on the government of Namibia to speedily implement the much awaited Access to Information Bill. This will go a long way to preventing access to information not only for journalists but also members of the general public.

Interviewees from the civil society organisations indicated that there are some youth, religious and women's organisations, which have been branded as 'extremist' and 'enemies of the state'. Similarly, Links (2018) observes that this was confirmed by official from NCIS during a Children and Cybersecurity Workshop in Windhoek, Namibia.

There was a strong feeling that the Landless Peoples' Movement (LPM), which has been at the forefront of lobbying government to undertake a radical approach to land redistribution, could be part of the targets of communication surveillance. Although no concrete evidence exists, interviews with members of civil society organisations suggested that this trend could not be entirely ruled out. The LPM was formed after former SWAPO cadres, Bernadus Swartbooi and Pendukeni Iivula-Ithana, were fired from the party under unclear circumstances. Their main grievance has been the issue of ancestral land, which they claim must be returned to the rightful owners (certain Namibian tribes). The movement has since registered[25] with the electoral commission with a view to participate in the November 2019 general elections.

Similarly, the Namibia Economic Freedom Fighters (NEFF), a copycat of the South African Economic Freedom Fighters (EFF), could also be part of the growing list of surveillance targets in post-apartheid Namibia. This was revealed during our key informants interviews with activists in Namibia. The party was formed in June 2014, and it has close links to the South African Economic Freedom Fighters. It is led by Epafras Jan Mukwilongo.

Another organisation, which is often viewed as too "radical" and "revolutionary" in its approach is the Affirmative Repositioning (AR), which like NEFF, has adopted direct action and cyber-activism in terms of pushing for the improvement of the socio-economic conditions of urban youth (Becker, 2016). It was formed in November 2014 by Job Amupanda, Dimbulukeni Nauyoma and George Kambala. The movement uses social media platforms to mobilise residents to apply for erven (small residential land titles) from municipalities. Due to thousands of youth submitting their forms on the same day, these activities have the character of mass demonstrations.

5.4 The adequacy of oversight of communication surveillance in Namibia

One of the major problems registered by this study was that Namibia does not have adequate oversight mechanisms to enable legitimate, proportionate and necessary communication surveillance in the digital age. The current legislative regime as evidenced by the Namibia Central Intelligence Services Act of 1997 and the Communications Act of 2009 (especially part 6, section 70-77) are not fit for purpose. For instance, part 6 of the Communications Act gives sweeping powers to the Director General of NCIS and imposes intermediary liability on the part of telecommunication service providers.

24 https://www.namibian.com.na/185296/archive-read/Geingob-urged-to-pass-info-law-to-prove-transparency

25 https://www.lelamobile.com/content/78784/LPM-now-a-political-party/

Interviews with regulatory officials in Namibia revealed that at the present moment, the ministry and the regulator do not regulate the surveillance of private citizens. One of the respondents observed that:

"The framework for the interception of telecommunications services is contained in Part 6 of the Communications Act (No. 8 of 2009), which has not yet been commenced."

Although part 6 of the Communication Act of 2009 has not yet been implemented credible reports suggest that interception centres are already in operation (UN UWR, 2016). This raises concerns as to which law is being used at present to regulate the operations of these monitoring and surveillance centres.

Furthermore, our key informants explained that the Communications Act in general and part 6 of the Communications Act in particular does not deal with data protection. Another key respondent explained it as follows:

"There is a difference between interception and data protection. However, Namibia does not have a data protection law at the moment. The power to enact legislation on data protection lies with the Minister of ICT and CRAN as an enforcer of the law will only wait for the Minister to put this in motion".

With regards to part 6 of the Communications Act of 2009, our key informants also highlighted that the Authority is not aware of when this piece of legislation will come into force.

5.5 How is the civil society pushing back against surveillance creep in Namibia?

Civil society organisations in Namibia have yet to mount a significant push back against the pro-surveillance policy and regulatory initiatives. Because of limited public awareness on the extent of surveillance creep, there have been limited attempts by the civil society in Namibia to mount resistance against the normalisation of surveillance in everyday life. Interviewees also pointed out that very few organisations were working on the matter.

The Namibia Media Trust has published press statements condemning the idea of launching a single internet gateway system. The Institute of Public Policy Research has published policy briefs on surveillance and also held public events to raise awareness on what they call the "rise of the surveillance state". Civil society have also pushed for the crafting of the Access to Information and Data Protection laws in order to protect citizens from arbitrary surveillance practices. Some of the respondents had this to say:

"Every citizen and resident needs to be guaranteed privacy… The rate at which government is progressing towards them is relatively low. It is not clear whether government is equally keen on ensuring and guaranteeing privacy"

(Journalist).

Respondents from the civil society raised pertinent concerns with regards to the proposed26 cyber-security bill. They observed:

"We have raised concerns with sections of the Cyber-security Bill that give security agents access to private data in a manner that we think is excessive. We asked that anything to do with access to data of private citizens be authorised by a court law rather than be placed in the hands of institutions such as security agents. To a great extent, we found that particular clause of the cyber security bill problematic and a threat to human rights."

(Member of civil society organisation)

26 https://www.namibiansun.com/news/serious-flaws-in-cybersecurity-bill2018-02-12

"We believe in cyber-security but we also believe that the Bill that will be tabled before parliament later this year must guarantee the privacy of citizens. For this reason, we are pushing that a Privacy law be also passed at the same time this Bill comes into law, and we have had such deliberations with the Ministry of Information and Communication Technology to try and have them to understand the risk there is to the privacy of citizens".

(Member of civil society organisation)

Because of the nature of their work and the role they play as watchdogs, journalists and civil society organisations are vulnerable to monitoring by the government which can take the form of communication surveillance. When journalists engage with their sources, it's important to guarantee privacy and confidentiality to them. That is why in the past, media advocacy organisations like NMT and MISA organised training workshops for journalists in order to try and reduce the level of risk associated with digital surveillance.

There is evidence that the state is taking civil society's push against the surveillance seriously as evidenced[27] by the withdrawal of the 'Spy Bill' and the foot dragging approach with regards to the launch of the single internet gateway system and mandatory SIM card registration.

The government is also very sensitive in terms of endangering their record on press freedom and freedom of expression largely because of its ranking globally and on the continent in terms of media freedom issues. The country will be in a similar quandary to South Africa, where it is resistant to making significant concessions to lessen inequality, yet is has a relatively freer and open political culture. This means that there is something about the Namibian social fabric and political situation that is quite durable and less susceptible to surveillance creep.

27 https://neweralive.na/posts/namibians-will-not-be-spied-on

6. Conclusion and Recommendations

This mapping study has found that there are serious concerns of the development of the surveillance infrastructure in Namibia. There are a number of reasons, which have been proffered to explain the adoption of several policy and legislative frameworks, which are inclined towards state surveillance. Increased intra-party conflict, fervent demands for land reform, ethnic tensions and rising unemployment figures especially amongst the youth (according to the Namibia Labour Force (LFS) (2019), the youth unemployment rate in Namibia stands at 44.8%) have raised public safety and order issues within the security establishment.

This study has discussed the basis upon which surveillance concerns have been raised in Namibia especially with regards to the acquisition of surveillance technologies, the government monopoly in the telecommunication sector, the role of Chinese telecommunication companies in the Namibian telecommunications sector, the push for single internet gateway system, the talk of mandatory SIM card registration and the reluctance to roll out the data protection and access to information laws.

Most of these policy interventions adopted over the last few years have raised concerns about the increasing powers to conduct surveillance, the omission to establish and enforce prior judicial authorisation, and the broader powers of intelligence agencies without oversight. Interviews with key informants have corroborated findings from the qualitative policy and document analysis.

6.1 Recommendations

The Government of Namibia

The following recommendations are made for the government:

- The government of Namibia should not implement mandatory SIM card registrations, as such blanket data retention infringe on the privacy of citizens and makes it difficult for people to communicate anonymously.
- The government should recognise and take steps towards compliance with international human rights law and standards by ensuring the application of the following principles to communication surveillance, namely legality, legitimacy, necessity, adequacy, proportionality and respecting process of authorisation from a competent judicial authority; due process, user notification, transparency, public oversight and respect for the integrity of communication and systems as well as ensuring safeguards against illegitimate access and right to effective remedy;
- There is an urgent need for the Ministry of Information and Communication Technology to adopt a comprehensive data protection law that complies with international human rights standards and establishes an independent data protection authority;
- Security breaches of personal data which directly threaten the right to privacy of its citizens have to be investigated, followed by necessary measures to ensure those responsible are sanctioned and case of recognised violations, victims have access to redress.
- It is essential that the government takes the steps necessary to ensure the protection of its citizens' personal data when engaging with third parties. These provisions provide the framework to allow authorities to conduct mass surveillance of its citizens. In order to comply with international human rights laws and standards, laws regulations communication surveillance must respect the principles of legality, proportionality and necessity, including by defining whose communications are to be intercepted, which types of communication can be intercepted, and for what purpose.
- The operations of interception centres must not take place outside of part 6 of the Communication Act of 2009. The Minister of ICT must publish in the Official Gazette the implementation of part 6 as reform the reform process.
- The government should publicly disclose details of the scope and scale of its surveillance activity at the level of clarity and granularity espoused by the Necessary and Proportionate Principles, including the deployment of the IMSI catchers (a technology with the capacity to enable mass communication surveillance).
- The Namibia Central Intelligence Service Act, 1997 (Act No. 10 of 1997) should be urgently amended so that it is in sync with the international best practices with regards to incorporating the Necessary and Proportionate Principles[28].
- The government of Namibia should ensure that the oversight body of intelligence is independent and granted sufficient powers and resources, both human and financial, to fulfill its mandate (see also UN good practices on oversight institutions in the appendix section). The Fundamental Rights Agency of the European Union (FRA) (2015) provides some innovative oversight mechanisms for surveillance by intelligence services. The report argues that oversight should be a combination of executive control, parliamentary oversight, judicial review and expert bodies.

28 https://necessaryandproportionate.org/principles

The Parliament of Namibia

The following recommendations are made for the Parliament of Namibia:

- The Parliament of Namibia should amend part 6 of the Communications Act of 2009 to ensure that people whose communications have been intercepted are informed after the completion of investigations, or if the designated judge refuses to grant an interception direction. Part 6 of the Communications Act of 2009 must be reformed in order to meet international and regional frameworks on monitoring and interception of citizens' information and metadata;
- The Parliament and the Namibian Police Force must investigate all unlawful communication surveillance activities by Namibian security agencies that have been reported by the media and other actors; the necessary measures to ensure access to redress in case of violations should be taken;
- The parliamentary committee on security and defence should be given powers to hold intelligence agencies like NCIS to account.
- The Parliament of Namibia should appoint a designated judge to deal with issues of monitoring and interception of communication over telecommunications networks. This can take the form of the RICA judge[29], as is the case in South Africa. In the South Africa context, if law enforcement agencies want to intercept someone's communication in real time, they first have to apply for a warrant from a special judge who is appointed by the President. If the judge approves their application and provides a warrant, this warrant can force any telecommunications company or internet service provider to help the agency intercept the communication of the user or users.
- The parliament of Namibia must ensure that the appointed judge should outline in his/her annual report how many directions resulted in arrests and convictions.

Communication Regulatory Authority of Namibia

- CRAN, the regulatory authority, should not fall under the authority of the Minister of Information and Communication Technology but it should be truly independent and report to the Parliament.
- The regulatory body must ensure that all telecommunication operators produce and publish periodic transparency reports with information such as the total number of each type of request, broken down by legal authority and requesting State actor, be it an individual, government agency, department, or other entity, and the number of requests under emergency procedures; the total number and types of responses provided (including the number of requests that were rejected); total numbers for each type of information sought; the total number of users and accounts targeted; total number of users and accounts affected; total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended.

29 https://www.biznews.com/undictated/2018/03/09/how-rica-is-totally-failing-in-sa

Civil Society Organisations

The following recommendations are made for civil society:

- There is a need to capacitate civil society organisations in Namibia in terms of the impact of communication surveillance. This can take the form of capacity building workshops on communication surveillance and surveillance technologies
- A broad-based coalition of organisations must be formed in order to tackle the issues of digital rights and surveillance head-on in the Namibian context.
- CSOs working the area of freedom of expression and media advocacy have the capacity to raise public awareness on the harmful effects of communication surveillance in post-apartheid Namibia.
- There is room for CSOs in Namibia to partner with other regional organisations in Zimbabwe, Malawi, Zambia and Swaziland, which are rolling out a campaign against the normalisation and institutionalisation of communication surveillance in the region.
- The proposed coalition can also rope in other players in the private sector, academia, journalists, trade unionists and community activists interested in communication surveillance issues.
- CSOs must strategically lobby for the urgent reform of the Communications Act of 2009, the NCIS Act of 1997, the introduction of Access to Information and data protection laws. They can take advantage of the government's appetite to introduce a revised version of the cybersecurity, data protection and access to information laws to lobby for progressive clauses.
- CSOs in Namibia must roll out public campaigns aimed at conscientising The envisaged coalition should also make the general public conscious of the violations of the right to privacy (amongst others) associated with mass communication surveillance in Namibia.
- CSOs must also focus on training their constituencies on various tools available which enable them to circumvent the dangers of mass and targeted surveillance.

The Media

The media must play an informative and educative role with regards to raising public awareness about the harmful impacts of communication surveillance.

Research and Academic Institutions

Funding must be made available so that research and academic institutions can conduct quantitative and qualitative baseline studies to ascertain the extent of surveillance amongst key constituencies, such as student activists, trade unionists, lawyers, opposition political parties, journalists and civic activists in Namibia. This information will form the basis for advocacy and campaigns around the prevalence of mass communication surveillance in Namibia. Research findings should be released publicly to build public awareness of the extent of mass communication surveillance.

Appendix

Figure 5: UN Good Practices On Oversight Institutions

UN good practices on oversight institutions

Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law, the effectiveness and efficiency of their activities, their finances and their administrative practices.

Practice 7. Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations and have full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses and obtaining documentation and other evidence.

Source: UN, Human Rights Council, Scheinin, M. (2010)

Figure 6: Standards for Oversight and Transparency of National Intelligence Services

Standard 1: Intelligence services need to be subject to oversight that is complete. This means it should be complete in terms of: a) the oversight body: the government, parliament, the judiciary, and a specialised (non-parliamentary, independent) commission should all play a role in oversight; b) the moment of oversight: prior oversight, on-going oversight, and after-the-fact oversight, and c) the mandate of oversight bodies: reviews of lawfulness and effectiveness.

Standard 2: Oversight should encompass all stages of the intelligence cycle. Surveillance involves different stages, including the collection, storage, selection and analysis of data. As all these stages amount to an interference with the right to privacy, these separate stages should be subject to oversight.

Standard 3: Oversight of the intelligence services should be independent. In this context, this means independence from the intelligence services and the government. Judicial oversight offers the best guarantees of independence. Therefore, it is preferable to involve the judiciary in the oversight on secret surveillance and data collection.

Standard 4: Oversight should take place prior to the imposition of a measure. In the field of secret surveillance of communications, especially by means of sophisticated technologies now associated with untargeted surveillance, the risk of abuse is high and abuse can have harmful consequences, not only for individual rights but also for democratic society as a whole. Therefore, prior independent oversight on the application of surveillance and collection

...continued

Standard 5: Oversight bodies should be able to declare a measure unlawful and provide for redress. Prior and on-going oversight bodies for intelligence services should have the power to prevent or end a measure imposed by intelligence services and oversight bodies should have the power to declare a measure unlawful after the fact and provide for redress.

Standard 6: Oversight should incorporate the adversary principle. The 'adversary principle' is a basic rule of law principle. Where secrecy is necessary, this can be implemented by the appointment of a special advocate who defends the public interest (or the interest of affected individuals). As a result, some form of adversarial proceedings would be introduced without the secrecy of measures to be imposed being jeopardised.

Standard 7: Oversight bodies should have sufficient resources to perform effective oversight. This standard includes the attribution of the necessary equipment and staff, resources in terms of information and technical expertise. This also contributes to their independence from the intelligence services and the government.

Standard 8: Intelligence services and their oversight bodies should provide layered transparency. This means that: a) the individual concerned, the oversight bodies, and civil society are informed; b) there is an adequate level of openness about intelligence activities prior to, during and after the fact and c) notification, aggregate statistics, working methods, classified and detailed information about operations, and general information about what will remain secret under all circumstances is provided.

Standard 9: Oversight bodies, civil society and individuals should be able to receive and access information about surveillance. This standard more or less mirrors the previous one. Clear legislation on receiving and accessing information about surveillance must provide a framework for oversight and support public scrutiny of the surveillance powers.

Standard 10: Companies and other private legal entities should be able to publish aggregate information on surveillance orders they receive. Organisations should be able to disclose aggregate information publicly about orders they receive directing them to provide information to the government. They should be able to make more detailed/ confidential information available to oversight bodies.

Source: University of Amsterdam, Institute for Information Law, 2015: pp. i-ii.

7. References

Bauman, Z, and Lyon, D. (2013). *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

Becker, H. (2016). Namibia's moment: youth and urban land activism. Review of African Political Economy website, http://roape.net/2016/01/18/namibias-moment-youth-and-urban-land-activism/.

Bertelsmann Stiftung Report. (2018). Namibia Country Report. Retrieved on the 22nd of May 2019 from https://www.bti-project.org/en/reports/country-reports/detail/itc/nam/itr/esa/.

Big Brother Watch, (2018). The State of Surveillance in 2018. United Kingdom. Retrieved on 23 May 2019 from https://bigbrotherwatch.org.uk/wp-content/uploads/2018/09/The-State-of-Surveillance-in-2018.pdf.

Chutel, L. (May 25, 2018). China is exporting facial recognition software to Africa, expanding its vast database. Retrieved on the 21st of June 2019 from https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/.

Dahir, A. L. (2018, January 30). China "gifted" the African Union a headquarters building and then allegedly bugged it for state secrets. Retrieved on the 6*th* of May 2019 from https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/.

Dencik, L. (2015). "The Advent of Surveillance Realism." JOMEC@Cardiff University. Accessed April 21 2019 from http://www.jomec.co.uk/blog/the-advent-of-surveillance-realism-2/.

Duncan, J. (2014). The Rise of the Securocrats: The Case of South Africa. Johannesburg: Jacana Media.

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

Duncan, J. (2016). Putting political economy back into struggles against communications surveillance: lessons from South Africa. Paper produced for the 'Memory, commemoration and communication' IAMCR 2016 Conference in Leicester, UK, July 27–31, 2016.

Emvula, T. (2017, August 18). Why a single Internet/Telecoms Gateway is a bad idea? *The Namibian*.

Ferguson, A.G. (2017). Policing Predictive Policing, 94 Wash. U. L. Rev. 1109 (2017). Available at: https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5.

Fidler, D. P., (ed.). (2015). *The Snowden Reader*. Bloomington: Indiana University Press.

Freedom House. (2017). Freedom on the Net-Zambia. Retrieved on the 2nd of April 2019 from https://freedomhouse.org/print/47749.

Gallagher, R. (2015, July 6), Twitter Post, 1:10 PM, http://bit.ly/1OGeQoW.

Gow, G.A and Parisi, J. (2008). Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones. *Bulletin of Science, Technology & Society* 28(1): 60–68.

Greenwald, G. (2014, May 13). *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State*. London: Hamish Hamilton.

Greenslade, R. (2013, August 19). How Edward Snowden led journalist and film-maker to reveal NSA secrets. Retrieved on the 2nd April from https://www.theguardian.com/world/2013/aug/19/edward-snowden-nsa-secrets-glenn-greenwald-laura-poitras.

GSMA. (2016, April). Mandatory Registration of prepaid SIM cards: Addressing challenges through best practice. Retrieved on 25 June 2019 from https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf.

Hammarberg, K, Kirkman, M and de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. *Human Reproduction*, 31(3): 498–501.

Human Rights Watch. (2014). With Liberty to Monitor all: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy. Washington DC: Human Rights Watch.

Friedrich Ebert-Stiftung. (2018). African Media Barometer-Namibia 2018. FES Media, Windhoek.

Lee, D. (2019). WhatsApp discovers 'targeted' surveillance attack. Retrieved on 7 May 2019 from https://www.bbc.com/news/technology-48262681.

Links, F. (2019). Spying on Speech. Democracy Report, Special Briefing No.28, June 2019. Retrieved on 7 May 2019 from https://ippr.org.na/wp-content/uploads/2019/06/IPPR-surveilance-web.pdf.

Links, F. (2018, February 16). The rise of the Namibian surveillance state (Part I). *The Namibian*.

Links, F. (2018, March 2). Surveillance Overreach: The rise of the Namibian surveillance state (Part II). *The Namibian*.

Links, F. (2018, March 15). The rise of the Namibian surveillance state: Part 3. *The Namibian*.

Lyon, D. (2001). *Surveillance Society*. Buckingham and Philadelphia: Open University Press.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Mare, A. (2018). Politics as usual? Facebook, political campaigning and contacting practices during the 2013 Zimbabwe's harmonised election. African Journalism Studies, 39(1): 90–110.

Mare, A. (2016). Facebook, Youth and Political Action: A comparative study of Zimbabwe and South Africa. An unpublished Ph.D Dissertation submitted at Rhodes University, Grahamstown, South Africa.

Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review*, 6(2). DOI: 10.14763/2017.2.692.

Privacy International. (2015). The Right to Privacy in Namibia: Stakeholder Report on Universal Periodic Review 24th session-Namibia. Submitted by Privacy International June 2015. Retrieved on the 29th of May 2019 from https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf

Radwin. (December 8, 2016). Police in Namibia Boost Safety with RADWIN's Video Surveillance Network. Retrieved on the 20th of June 2019 from https://www.radwin.com/press-room/police-in-namibia-boost-safety-with-radwins-video-surveillance-network/.

Right2Know Campaign. (2016). The Surveillance State: Communications surveillance and privacy in South Africa. Cape Town: Right2Know Campaign.

Schauer, F. (1978). *Fear, Risk, and the First Amendment: Unraveling the 'Chilling Effect'*. Boston University Law Review, 58, 685–732.

Schwab, K. (2016). *The Fourth Industrial Revolution*. Crown Business. World Economic Forum.

Sidhu, D.S. (2007). The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans, 7 U. Md. L.J. Race Relig. Gender & Class 375. Retrieved from http://digitalcommons.law.umaryland.edu/rrgc/vol7/iss2/10.

Tendi, B. (2016). State intelligence and the politics of Zimbabwe's presidential succession. *African Affairs*, 115(459): 203–224.

Tjitemisa, K. (2018 November 14). Shaningwa tired of teams Harambee and Swapo. https://neweralive.na/posts/shaningwa-tired-of-teams-harambee-and-swapo.

van Dijck, José. (2014). "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology." *Surveillance & Society* 12 (2): 197–208.

Xinhua. (2018, November 27). Huawei, Namibian mobile company commemorate decade partnership. Retrieved on 8 May 2019 from http://global.chinadaily.com.cn/a/201811/27/WS5bfd0497a310eff30328b56b.html.

Wahl-Jorgensen, K., Hintz, A. Dencik, L., & Bennett, L. (2017) Introduction, *Digital Journalism*, 5(3): 256–261.

York, J. (2014). Communications surveillance in the digital age: The harms of surveillance to privacy, expression and association, Global Information Society Watch 2014.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Profile, New York.