The growth of military-driven surveillance in post-2000 Zimbabwe

Allen Munoriyarwa

May 2021

The Media Policy and Democracy Project

exploring how the media can work better for society

The growth of military-driven surveillance in post-2000 Zimbabwe

Allen Munoriyarwa

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

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

May 2021

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

List of Acronyms

CCTV	Closed Circuit Television
CCTV	Closed Circuit Television
CIO	Central Intelligence Organisation
CSOs	Civil Society Organisations
DSZ	Digital Society of Zimbabwe
HRL	Human Rights Lawyers
ICA	Interception of Communication Act
ICTs	Information and Computer Technologies
IMSI	International Mobile Subscriber Identity
ISPs	Internet Service Providers
JOC	Joint Operations Command
MISA	Media Institute of Southern Africa
MNOs	Mobile Network Operators
NGOs	Non-Governmental Organisations
PISI	Police Internal Investigations Services
POTRAZ	Post and Telecommunications Regulation Authorities of Zimbabwe
RGMSI	Robert Gabriel Mugabe School of Intelligence
ZANU-PF	Zimbabwe African National Union-Patriotic Front.
ZDF	Zimbabwe Defence Force
ZEC	Zimbabwe Electoral Commission
ZLHR	Zimbabwe Lawyers for Human Rights
ZMI	Zimbabwe Military Intelligence
ZNA	Zimbabwe National Army
ZRP	Zimbabwe Republic Police

Table of Contents

Executive Summary 1

Summary of key findings 2

The structure of this report 3

The birth and character of post-coup Zimbabwe: A brief synopsis 4

Scope and aims of the study 6

Rationale for the research project 6

Methodological issues 7

Zimbabwe's digital surveillance architecture 9

The ZDF's communication surveillance capabilities 14

Enablers of ZDF's surveillance capabilities 16

The political economy of surveillance:
The actors and interests within ZNA 17

Concluding remarks 24

References 29

Executive Summary

Zimbabwe's long-time ruler, Robert Mugabe, was deposed by a military coup in November 2017. This was a culmination of a long succession feud between Mugabe and his erstwhile ally, Emmerson Mnangagwa, now the current president. Eventually, the military sided with the latter. The deposition of Mugabe highlighted the centrality of the military in Zimbabwe's post-colonial politics. It was clear that the gun would lead the politics. The military had once more become the arbiter of Zimbabwe's politics, like they did in 2008, when they pushed Mugabe to refuse defeat. That the Zimbabwe Defence Force (ZDF) is a powerful political entity is now beyond doubt (Tendi, 2019). The strength of the military has been enabled by a number of factors. These include, access to financial resources through generous budgetary allocations from the treasury. The military has also benefitted from loans and grants, backed by the central government, from other countries, especially China, Iran and Russia. Recently, the ZDF has been involved in (military-driven) digital surveillance. Existing documents and interviews have shown that the ZDF has accumulated digital surveillance technologies that it has used against citizens. This is despite the absence of constitutional provisions allowing the entity to undertake the surveillance of citizens outside a war situation or emergency. This, therefore, constitutes a "mission creep", as it is against the country's own laws and the purported reformist mindset of the current rulers.

Military-driven surveillance raises specific issues with regards to human rights. Because it is not provided for in the constitution, there is now an obvious danger that this practice is politicised. When it is politicised, it can lead to suppression and repression of anti-government voices. This in itself is a human rights abuse issue that cannot be tolerated in countries calling themselves democracies. There are also other questions. For example, what happens to the data after use? The structure of the ZDF makes it incapable of practising transparent and accountable surveillance, given the absence of a clearly defined constitutional mandate. More so, global standards of surveillance (see for example, the United Nations Human Rights Office Guidelines 2017) have devolved two very important mechanisms around digital surveillance of people. First, post-surveillance notification is important. This practice ensures that, as a right, targets of surveillance are informed post-facto. Second, both judicial authorisation and oversight have become key pillars of surveillance practices in the post-Snowden period. In the Zimbabwean case, these two crucial elements are missing. This confirms that surveillance in the country is a political, not a crime-fighting, practice. Thus, one can argue that post-coup Zimbabwe has become one side of the same coin with the Mugabe regime. The difference, based on the evidence, might be that post-coup Zimbabwe has witnessed hardening digital authoritarianism driven by the military. A heavy reliance on China might, possibly mean data ends up in China, in exchange for surveillance technology, giving China an opportunity to use the data to train its technologies.

Summary of key findings

In this section, I summarise what the evidence that will be provided in the coming sections points to. The summary provided here comes from the two sources of data utilised for this research: namely, document analysis and interviews (see the methodology section below).

1. Zimbabwe Defence Forces' surveillance capabilities and practices are expanding

The Zimbabwe Defence Force's (ZDF) capabilities have grown in both public space surveillance and cyber-communication surveillance. The growth is aided by the Chinese government, which has advanced both the surveillance technology and "soft loans" for the purchase of surveillance technologies. Chinese start-up technology companies like Huawei, HikVision and CloudWalk have also been central in providing the Zimbabwe state with surveillance technologies like CCTV cameras and facial recognition technologies. There are also new players central to the realisation of Zimbabwe's surveillance intentions. These are Iran and Russia, who have also provided Zimbabwe with these technologies, including other military hardware.

2. The nature of the ZDF's surveillance capabilities

Numerous ZDF units, especially the MI and Signals Unit, are accumulating a vast array of surveillance equipment that allows them to undertake public space and communication surveillance. The MI is the principal surveillance unit of the ZDF. However, according to respondents, the military has developed other "sub-units" within many of its branches that have been equipped to undertake digital surveillance. These include the Signals Unit and some units within the special forces of the ZDF. According to respondents, and evidence already in documents and mainstream news, the accumulation includes the following:

(a). The ZDF staff college in Harare, in liaison with Transsion, a Shenzhen-based artificial intelligence (AI) company, is experimenting with facial recognition technology that recognises dark skin colour. The ZDF is actively importing this technology.

(b). The ZDF has email hacking capabilities, imported from Iran, that to our knowledge have been used at least twice in Zimbabwe since 2000.[1] Respondents were not sure of the details of the type of hacking equipment the military possesses.

(c). The ZDF is importing facial recognition technology from CloudWalk, a Chinese AI company.

(d). The ZDF has imported IMSI catchers from Iran that, according to sources, have recently been used to track political opponents.[2]

(e). The ZDF is importing CCTV cameras from HikVision, another Chinese company. Some of these cameras have been "donated" to city councils for use in urban areas and highly secure areas. No one knows how and where the footage collected by these surveillance technologies is stored, by whom, or for what purposes.

(f). There is an agreement between the ZDF and China's Ministry of State Security (MSS). that provides for China's specialised units in network intrusion to help the ZDF build such capabilities at Robert Mugabe Defence University in Harare. Under the agreement, Chinese Information, Operations and

1 Elizabeth Macheka-Tsvangirai, wife of the late MDC leader Morgan Tsvangirai, and Pius Ncube, then Archbishop of the Roman Catholic church, both had their email surveilled over a long period of time. See: https://www.theguardian.com/world/2007/jul/21/zimbabwe.chrismcgreal.

2 The recent case of Job Sikhala can be followed here: https://zimbabwe.shafaqna.com/EN/AL/800114.

Information Warfare (CIOIW) units as well as Chinese cyber-specialists are helping ZDF personnel in the matter of cyber-information investigations and related areas. These two Chinese organisations – the MSS and CIOIW – are known for their digital surveillance capabilities, which have been flagged in Canada, the UK, the USA and Australia (see Gramer, Detsch & Haverty, 2020; Rohrlich, 2020).

3. Current surveillance practices in Zimbabwe are unnecessary and unjustified

There is no specific threat defined by the state, as is necessary, to warrant surveillance. Evidence shows that most of the surveillance practices by the state agencies are political, because they target outspoken opponents of the regime as the report will show. They are meant to suppress opponents of the ruling party ZANU-PF, and within ZANU-PF itself, surveillance targets opponents of the current president. It is, hence, factional. There is no logical justification (such as fighting crime) for the surveillance by the state of its targets; the rationale is purely political suppression.

4. Attenuation of other agencies

The surveillance practices of the ZDF have, consequently, attenuated other agencies with a legal mandate to practice surveillance. The ZRP, the CIO and the ZIMRA have constitutional mandates to practice surveillance (see the constitution of Zimbabwe). Yet, their mandate has been eclipsed by the growing role and influence of the ZDF in this regard.

5. ZDF's mission creep

As a result of the above, it is concluded that the surveillance practices of the ZDF constitute a mission creep because the army has no legal mandate to practice surveillance. It is important to note that generally, the military in Zimbabwe have no arresting powers, let alone powers of investigation. This means their surveillance of civilians, outside a conflict period, or a declared state of emergency, constitutes a sharp violation of rules and a serious mission creep.

The structure of this report

This report is structured as follows. In the next section, I provide a brief context on the birth and character of post-coup Zimbabwe. That will be followed by a scope of the study, a justification of this research, and the methodology adopted. The next two sections outline the legal architecture governing surveillance in the country and give a synopsis of the architecture of surveillance institutions provided for in the country's constitution.

The bulk of the report presents the findings of the project and conclusions that can be drawn from them. Lastly, key policy recommendations are provided for critical constituencies involved in surveillance in Zimbabwe.

The birth and character of post-coup Zimbabwe: A brief synopsis

Since its independence in 1980, Zimbabwe has been a semi-authoritarian regime (Makumbe, 2009; Sachikonye, 2011; Masunungure, 2020). Semi-authoritarian regimes occupy the grey area between fully-fledged authoritarian regimes and democracies (Ottaway 2013). In semi-authoritarian Zimbabwe, the military falls under the regime's "menu of manipulation" – manipulated for political survival. There is a rhetorical acceptance of liberal democracy and formal democratic institutions that are made to exist in attenuated form (Ottaway, 2013).

The current regime in Zimbabwe, calling itself the "Second Republic", came into power in November 2017 after a military-assisted deposition of the long-time ruler, Robert Mugabe. The coup that removed Mugabe provided fodder for frequent accusations that the military was a ruling party organ. Moreover, it was a manifestation of the army's involvement in the factional politics of the ruling Zimbabwe African National Union-Patriotic Front (ZANU-PF).

The removal of Mugabe from power was followed by a massive re-alignment of ZANU-PF party politics. Top ruling party positions and cabinet ministries were dished out to former and serving senior military personnel. Ambassadorial roles were also awarded to former military personnel. The current president – Emmerson Mnangagwa – is said to have very close ties with the Chinese (*The Zimbabwe Independent*, 2018). His close relations with the Chinese military helped him depose Mugabe (see *The Zimbabwe Independent*, 2017). Since the fall of Mugabe, the Zimbabwe military has gained a great deal of influence in security issues, more than that of the Central Intelligence Organisation (CIO) and the Zimbabwe Republic Police (ZRP) (ZimCoDD, 2018). Their level of influence in government has also increased, with deployments of current and former military commanders in civilian positions having peaked since the fall of Mugabe (Ruhanya, 2019). The military is increasingly usurping the powers of civilian security institutions – the ZRP and the CIO in particular (Dhlela, 2019). Perhaps the main reason for this usurpation of powers is that the military has become the present regime's most trusted security institution, having helped the current rulers to overthrow Mugabe. The police and the CIO are, arguably, still viewed with suspicion, as they fought in Mugabe's corner during the succession disputes leading to his overthrow. Tendi's (2019) research has shown how, during the coup that removed Mugabe, senior police officers, and sections of the police, like the Zimbabwe Republic Police Support Unit, had to be disarmed because their loyalty to the coup plotters was doubted. As a result, the ZDF became an influential institution in government (see Ruhanya, 2019). Human rights organisations and legal organisations (for example, Veritas, 2019) have asserted that the country has been effectively and totally militarised.

Evidence of this militarisation has also manifested in other intensified post-coup practices. For example, senior military commanders have been appointed as directors and permanent secretaries in many civilian ministries, and military officers have been included in state commissions.[3] The "permanent" presence of the military personnel on police traffic duties underlines the extent to which this militarisation has been completed. In late 2019, the Zimbabwe Constitutional Court ruled that the involvement of military personnel as prosecutors

3 For instance, as of August 2020, the Minister of Health and Child Welfare is a former commander of the ZDF, the Deputy Minister is a retired colonel deployed to the ministry and a personal physician to the Minister. The permanent secretary in the same ministry is a colonel in the army, and a personal physician of the president.

was illegal.[4] This was after it was noted that serving and retired military officers had been seconded to the National Prosecuting Authority of Zimbabwe, a civilian institution.

The genesis of the complete politicisation and militarisation of the ZDF can be traced to the growing economic and political crisis in the country post-2000, when Mugabe was still leader. As the economy imploded, Mugabe found himself facing serious opposition from the country's largest labour movement – the Zimbabwe Congress of Trade Unions. Opposition to Mugabe's economic policies led to a broad-based political opposition being formed against ZANU-PF in September 2000. The new party was called the Movement for Democratic Change (MDC). Faced with declining political support and a profoundly divided political elite, Robert Mugabe had to resort to the mobilisation of state institutions that should, constitutionally, operate outside politics.

The fact that most of the senior officers in the military have a liberation war history, a liberation war largely driven by ZANU-PF, made it easy for the ruling party to revive these old ties and nostalgia amongst military men and women and completely capture them for the party's political survival. This explains why senior military personnel campaigning for ZANU-PF during elections instructed their juniors to vote for the ruling party and threatened opponents on behalf of ZANU-PF. In a way, the "Zanufication" of the military – turning the military into a ruling party organ for political survival – made the military an insecure and authoritarian institution with huge numbers of its officers developing attitudes that were no longer in harmony with their professional calling as a defence force. The process of politicising the armed forces was in tandem with ZANU-PF's rules of politics, but its consequence was that it destroyed the institutional integrity of the army.

In the post-coup era, senior police officers and senior intelligence personnel have been purged, possibly because of doubt in their loyalty to the new dispensation (Tendi, 2019). The lingering suspicion between the ruling administration and these key institutions has given room to the military gaining more power and authority in security issues (Ruhanya, 2019), and even in civilian spaces (Ruhanya, 2019). Emerging research (see Dhlela, 2019) shows that the military is building massive digital surveillance capabilities, amply funded by the state, with help from China (Dhlela, 2019; MISA, 2018). They are, for instance, involved in the establishment of a data centre (*Nehanda Radio*, 2019). The Zimbabwe Defence Act (Chapter 11:02), makes it clear that civilian surveillance and internal crime-fighting powers are vested in the hands of the ZRP and the CIO, unless during a declared emergency, when the military can join in. The involvement of the military raises pertinent questions about the rationale of their involvement and the current extent of this involvement. As has already been mentioned, the constitution of Zimbabwe does not provide for such involvement unless the country is facing a war or there is an internal insurrection. More so, under the country's constitution, the military have no arresting powers. This, therefore, raises questions like: what will they do with the data they collect if they cannot apprehend criminals and arraign them? Why are the institutions with the constitutional mandate to do so, like the police, not equipped to do so, and wrest this responsibility away from an institution that in the first place, should not be involved? These are the issues this report seeks to explore.

The active involvement of the Zimbabwe military in digital surveillance practices should be understood in the context of the ZDF finding a new role in the post-coup era, and the ZDF's attempts to consolidate the political power of the ruling party, ZANU-PF, by silencing opposition to it. ZANU-

4 The Constitutional Court of Zimbabwe ruled that the use of prosecutors from the ZDF in civilian courts is unconstitutional (see *Zimbabwe Law Officers' Association & Another v NPA & Others* (CCZ 1/19, Const Application No CCZ 32/14) [2019] ZWCC 01 (19 February 2019). Available from: https://zimlii.org/zw/judgment/constitutional-court-zimbabwe/2019/1

PF was left severely weakened after the coup as a series of purges eliminated senior party officials. Some members have been alienated for being pro-Mugabe. The military's active involvement in digital surveillance is hence supposed to be understood as part of its post-coup mission to use digital surveillance against political opponents in the ruling party. The military achieves this by weaving fear and securitisation into the practice of surveillance. These developments require interrogation.

Another notable feature of the post-2000 period has been the ruling regime's heavy investment in the Zimbabwe military. Since 2000, the military has enjoyed more funding than other government ministries despite, for example, the collapsing health and higher education sectors (ZimCoDD, 2018). The post-coup dispensation has increased the ZDF's synergies with other countries, chief amongst them being China, Russia and Iran, and has also further increased the budgetary allocation of the ZDF (ZimCoDD, 2018). It is against this background that this project seeks to explore the ZDF's growing digital surveillance practices since the year 2000 when a new political opposition was born and public dissent against the ruling party began to grow, and when elite disunity began to grow within the ruling party itself.

Scope and aims of the study

This study explores the growing culture of military-driven surveillance in Zimbabwe. It seeks to establish the "character" of the surveillance practices that the ZDF has been implementing, especially since the year 2000 when the Chinese, known for having established one of the most elaborate digital surveillance systems in the world, started collaborating with the Zimbabwe military. The study will focus on the following three major areas:

- The current capabilities of digital surveillance within the military
- The political economy of military-driven surveillance in Zimbabwe – that is, the powers, actors and enablers both within and outside the military establishment that are driving such digital surveillance practices
- The targets of military-driven surveillance in the Zimbabwean context.

Rationale for the research project

Several researchers (see Human Rights Watch, 2018; Media Institute of Southern Africa, 2018; Media Policy and Democracy Project Report, 2019) have pointed out that there is a growing culture of digital surveillance in post-2000 Zimbabwe. The MPDP (2019) report asserts that the ruling regime is afraid of a revolt by the youth, the opposition and Civil Society Organisations (CSOs) as the economic meltdown continues unabated. Thus, according to this report, digital surveillance has been a weapon in the arsenal of the state elite to suppress and repress revolt and protests. However, it is important to point out that the use of digital forms of surveillance as a substitute for the now all too banal physical surveillance is a growing global phenomenon (Calatayud & Vázquez, 2019). But in Zimbabwe, constituencies critical to democracy, like journalists, have pointed out that digital surveillance is growing, is especially targeted at investigative reporters, and is happening outside the legal provision (Munoriyarwa & Chiumbu, 2020). This is happening in a country where a lack of regard for human rights has been growing since 2000 (MPDP, 2019). Worse still, there is no well-coordinated response by CSOs to the growing threat of mass digital surveillance (MPDP, 2019).

This failure by CSOs to respond adequately to the state's surveillance practices comes at a time when the ZDF has become a very powerful, central arbiter of Zimbabwe's politics in the post-coup era. In addition, CSO's failure to adequately raise the issue of digital surveillance practices by the state has left a lacuna, which allows state agencies to operate with impunity and to intensify extra-legal surveillance. While MISA-Zimbabwe has been actively engaged in raising awareness on this issue, it has been the only organisation noticeably engaged on the issue. The need to establish the severity of these antidemocratic practices comes amidst three developments: (1) The growing militarisation of the society noted earlier; (2) heavy Chinese, Russian and Iranian involvement with the ZDF; and (3) the ZDF's heavy and visible involvement in civilian policing and prosecution duties. Taking cognisance of all these developments, it is pertinent, therefore, to explore military-driven digital surveillance in Zimbabwe by mapping out the trends, identifying the powers involved and the interests of the actors within the ZDF, as well as to identify the players behind the supply of these technologies.

Methodological issues

This research relies on two sets of data. It relies first on a document analysis, utilising credible mainstream news reports, reports by NGOs and CSOs, and commentaries by human rights bodies. However, it is important to point out that much of what exists on this subject is merely credible mainstream news reports. This is because the field of military-driven digital surveillance lies unresearched and hence there is no scholarship to rely on. This research therefore augments the document analysis with a set of eight (8) face-to face interviews. (see Table 1 below).

Researching the military in Zimbabwe is not an easy task. Even writing about it can have significant negative repercussions. The ZDF has developed a reputation as an unapproachable institution that abuses human rights. Even media houses find it difficult to obtain comments from the ZDF. The shooting of seven protesters during the 2018 election demonstrations did little to assuage this reputation.

Nevertheless, the participants in this study were a rich source of data around military-driven surveillance. Data collection was facilitated by one factor in particular – the growing economic decline of the country has resulted in great overall disillusionment. This has led to a measure of openness in the military that may have made respondents more amenable to participating in the study.

The respondents included former military personnel who had worked for the ZDF in either the Zimbabwe Military Intelligence (MI), a ZDF special investigative unit, or the Signals Unit (SU), known to be involved in surveillance. The sample also included a member of the ruling ZANU-PF, who served in different legislative and government committees where such issues were discussed. The respondents have all left these particular institutions, and most of them have migrated and settled elsewhere. They are indicated as respondents numbered from 1 to 8 for the sake of anonymity.

Table 1: Summary of the research respondents

Respondent	Previous position
Respondent 1	ZDF Signals Unit
Respondent 2	ZDF Special Investigative Unit
Respondent 3	Zimbabwe Military Police
Respondent 4	ZANU-PF Committee on Defence and Foreign Affairs
Respondent 5	Instructor: Military College
Respondent 6	ZDF Signals Unit
Respondent 7	Zimbabwe Military Police
Respondent 8	ZDF Special Investigative Unit

The legal framework of surveillance in Zimbabwe Zimbabwe is a signatory to a number of human rights protocols under international law that protect freedom of expression, privacy, including digital privacy.

The United Nations Human Rights Council (UNHRC) adopted a position in July 2012, affirming that the same rights that people have offline must also be protected online, in particular, "… freedom of expression, which is applicable regardless of frontiers and through any media of one's choice." The resolution, which China did not oppose, also "call[ed] upon all States to promote and facilitate access to the internet". While offering no specific guarantees, these international agreements set the tone regarding important principles like freedom from arbitrary and extra-legal surveillance by the state or private entities – practices that have a tendency of scaring people away from the online space (Fuchs, 2011). Zimbabwe is a signatory to these international resolutions, but the country has not sufficiently captured the letter and spirit of these agreements in its domestic legal jurisprudence. As Veritas (2019) notes, surveillance regulations in Zimbabwe seem to highlight the conflict between political interests and legal values, with the former intensively shaping surveillance regulations. For the Zimbabwe state, surveillance is a reaction to citizens attempting to organise, influence and advocate for change on online platforms. It is clothed, however, in the usual narrative of ensuring domestic stability and national security. The country's official narrative on surveillance as articulated by the military is that it is important to, "... fight hostile foreign forces and internal dissidents led by western sponsored opposition parties" (ZNA Commander, Edzayi Chimonyo, 12 May 2019). The Zimbabwe Interception of Communication Act (ICA) 2007 is a law that broadly regulates digital surveillance in Zimbabwe.[5] The law falls far below global standards, chiefly for the following reasons:

(1) It provides for ministerial oversight rather than judicial oversight. In other words, surveillance is authorised by a political appointee – a minister – giving rise to (often well-founded) fears of political surveillance, especially in a politically polarised country like Zimbabwe. It can thus be used against political opponents.

(2) In addition to the minister, heads of state security institutions, like the CIO and ZRP, can also delegate surveillance to other lower-level officials without necessarily getting court approval.

(3) It does not provide for post-surveillance notification, where targeted individuals are informed post-facto. This is a crucial internationally accepted mechanism of surveillance practices, ensuring that surveillance is not by and large a "black box", giving too much power to institutions.

(4) There is no provision in the statute on what happens to the data collected after surveillance, making it impossible for people to know what happens to their data. Human rights organisations (see Veritas, 2019; ZLHR, 2017), have criticised the law for fundamentally violating human rights, especially the right to privacy. Academic researchers (see Munoriyarwa & Chiumbu, 2020) have also noted that this surveillance law has a chilling effect on critical constituencies of society, the opposition, CSOs, and journalists. There is no provision for military-driven surveillance in the ICA. The involvement of the military is provided for under the Defence Act and the Presidential Powers (Temporary Measures) Act (Section 20:20 of the Zimbabwean Constitution). This is an Act that empowers the President to make regulations dealing with situations that have arisen or are likely to arise and that require to be dealt with as a matter of urgency; and to provide for matters connected therewith or incidental

5 The law is accessible here: http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf.

thereto. The Defence Act provides for civilian surveillance during war, or moments of armed insurrection. Outside these contexts, surveillance on civilians is illegal.

A new law is currently being debated in the legislature – the Cyber Security and Data Protection Bill (2019).[6] The Cyber Security and Data Protection Bill is meant to consolidate cyber-related offences and provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest. It will facilitate the creation of a Cyber Security Centre and a Data Protection Authority, and also provide for their functions, provide for investigation and collection of evidence of cybercrime and unauthorised data collection and breaches, and provide for admissibility of electronic evidence for such offences. One journalist said that, if passed into law, the bill "will create a technology-driven business environment and encourage technological development and the lawful use of technology" (email interview, 26 July 2020).

This particular proposed legislation has ignited fierce opposition among CSOs in Zimbabwe. The biggest concern raised by these groups is the conflation or amalgamation of cybersecurity and data protection into a single piece of legislation. This, they argue, is against best practice and will make it challenging to strike a balance between security concerns and digital rights. Such an "omnibus approach" created problems with the Access to Information and Protection of Privacy Act (AIPPA), which lumped together three complex issues such as access to information, media regulation and privacy. It has now been replaced by the Access to Information Act. The omnibus approach to the Cybersecurity and Data Protection Act is suspected to be a deliberate attempt by government to compromise the right to privacy. Organisations like the Zimbabwe Human Rights Lawyers' Association, for instance, propose that data access regulations and cybersecurity regulations should not be lumped together. Their reasoning is that lumping them together conflates two different issues and, hence, make it impossible for interested parties to, for instance, challenge one aspect of the provision (like challenging data retention laws, and not cybersecurity provisions lumped in that same law). They further argue that, in international best practice, the two should be treated differently, anyway.

6 The bill is accessible here: http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf.

Zimbabwe's digital surveillance architecture

The country has three intelligence agencies that have recently acquired, and are still in the process of amassing, surveillance capabilities, according to interviewees. These are the Police Internal Security Intelligence (PISI), the Central Intelligence Organisation (CIO) and the Zimbabwe Military Intelligence (popularly known as MI). Under the Zimbabwe Defence Act, the MI should act as an intelligence unit within the military and has no surveillance authority over civilians inside the country, except during a war, or as dictated by the president during a state of emergency. The same applies to the PISI; under the police act, it has no jurisdiction over civilian intelligence. Civilian intelligence is the prerogative of the CIO. But recent evidence (see for instance, *The Zimbabwe Independent*, 24 March 2019) shows a conflation of roles, with the CIO reportedly being torpedoed from its civilian intelligence focus, especially after the coup. The ousting of Mugabe weakened the CIO, which was viewed to be anti-Mnangagwa. The institution was purged, and most

of its senior personnel are said to have retired, or been forced to retire or redeployed to non-intelligence institutions (Nehanda Radio, 12 May 2018). These organisations now interact under the Joint Operations Command (JOC) structure that includes heads of these units, the President, military, police and prison commanders, and selected heads of civilian institutions. Zimbabwe's blurred line of party-military structures makes it difficult to foresee any future changes to the operations and leadership of these organisations, as this now depends entirely on the whims and caprices of the ruling party ZANU-PF. One police officer, who worked for PISI at one time, openly complained on a private radio station:

> *ZRP transfers are politicised. PISI section officers have their transfers reversed on political grounds. Following the recent transfers by ZRP to curb corruption in its departments, some members of the PISI had their transfers reversed on political grounds. This section specialises in political activities of other political parties and feeds the information to ZANU-PF for the smooth running of the party. This section is now like a ZANU-PF arm in the police service and is headed by Assistant Commissioner Nyakutsikwa, who caused a campaign of terror in all police provinces during the 2008 presidential run-off, whereby he went around all police camps threatening spouses and dependents of police officers to vote for ZANU-PF or risk a war (Former PISI member, speaking to Nehanda Radio, 12 May 2018).*

The PISI is an important organ of the ZRP. The fact that it has been politicised is dangerous on many grounds. First, it means a vital police unit is now dabbling in internal (political) party matters. This makes it susceptible to abuse. For instance, it can be used by that very political party to spy on its opponents. Second, it is common knowledge that state organs cannot and should not be political party organs as this goes against the principle of separation of powers.

These key intelligence institutions have been in constant flux, largely dictated by a realignment of politics within the ruling party. As some former members of these units said, in the process of being politicised, they have assumed local (political) responsibilities of ensuring citizens' political conformity to the ruling party, by intimidating them. This is in contravention of their national responsibilities like investigating and fighting sophisticated criminal syndicates and safeguarding national security. These current political practices reflect this party-intelligence relationship. It is in such a structure and in practice, that Zimbabwe's intelligence agencies mimic the Chinese ideology, which is structured for almost the same (political) purposes – to stamp down on opposition and criticism of the ruling communist party (see Lindsay, Cheung & Reveron, 2017 for an elaboration of Chinese surveillance architecture). Surveillance practices as well as current and proposed legislation in Zimbabwe clearly underline the ruling elites' phobia about opposition. Surveillance practices are exercised by different state institutions (like the police and military), with a strong (ruling) party influence. Consequently, like in the Chinese surveillance architecture, (see Richards, 2012), it is now difficult to distinguish between the decisions made within the intelligence services, and those made by political authorities because the lines have been blurred.

The CIO is divided into sub-units that have also constantly changed as a result of the changing leadership of the organisation, including, among others, counter-intelligence and internal intelligence units. However, some respondents argued that the counter-intelligence unit of the CIO is the one that sometimes coordinates surveillance activities with the MI. But, primarily, its role is to gather intelligence and threats emanating from outside the country – focusing mostly on detecting foreign threats like sabotage and assassinations, and

neutralising them. Respondent 7 noted, "It [CIO] has very limited capabilities of gathering foreign intelligence of value. This is why it has been used for other purposes like coordinating an elaborate surveillance system with the MI and PISI within the country rather than externally..." The respondent said that the CIO suffers from funding problems and has, over time, seen its ability to collect quality foreign intelligence diminish. Its reassignment to serve as an internal surveillance arm collaborating with the MI confirms the "bunker mentality" of the ruling party that sees enemies and threats everywhere. The military has gained the upper hand since the coup, and this may explain why other units remain underfunded.

One can also add to this, the general budgetary constraints of the country. Respondent 4 noted that these intelligence agencies have become stove-piped institutions – providing intelligence with no proper context simply because these processes are being driven by politicians, rather than qualified intelligence operatives. However, the existence of a JOC in which these institutions are represented perhaps shows that at different levels of policy and operations, intelligence is being shared, although the country, so far, has no known fusion centre where such cooperation is mostly evident. But, in a factionalised political atmosphere like Zimbabwe's, one can argue that cooperation between and among these agencies can be difficult as each of them vies for the attention of the elite members of the ruling party. Respondent 5 noted, for instance, that a deal to experiment with facial recognition technology was scuppered by the CIO as the agency felt it has been overtaken by the MI. The deal involved Cheetah Mobile, a Chinese start-up facial recognition company. Respondent 2 corroborated that a deal that included another Chinese start-up, Hanwang Technology, to experiment with gait recognition technology also died in its infancy as the agencies battled for control.

The ZDF's public space surveillance capabilities

According to the respondents, public space surveillance is one of the areas in which the ZDF's capabilties are growing. The ZDF has signed a number of agreements and deals with the Chinese government and technology firms, and the Iranian and Russian governments for the supply of public space surveillance technology. There are known agreements with HikVision, a Chinese company that manufactures cameras and CCTV. The ZDF is known, according to respondents, to receive such supplies from the company, and this dates back a long time. Respondent 5 said:

> *The agreement with Chinese companies like HikVision goes back to a few years ago. It's part of Zimbabwe-China megadeals. This should not surprise you because this information is in the public domain. It's read every day on the news when the leaders travel there. These are some of the so-called technological companies that they would be talking about investing in Zimbabwe.*

In July 2018, South Africa's *Daily Maverick* newspaper reported that the Zimbabwe government, through the ZDF, has entered into a deal with HikVision for the supply of public surveillance cameras and CCTV, "for the country to boost its security..." (n.p). Currently, public space cameras have been installed in Harare's central area – at the parliament building precincts and opposite Africa Unity Square, a place known for anti-establishment demonstrations. Respondents note that the ZDF, specifically the Signals Unit of the force, has been the driving force behind these installations, which have expanded vastly to include almost all the major cities of the country, like Bulawayo.

Because the ZDF does not have the constitutional mandate to do so, Respondent 2 noted:

> *It [the ZDF] hides by the ZRP and city councils to circumvent this legal loophole and to shield its involvement in the installations from the public ... it knows that it does not have that mandate.*

The installation of public space surveillance cameras and CCTV in government buildings should be the legal prerogative of the police, the CIO and city councils. But, as Respondent 3 noted, the ZDF has become involved for a number of reasons:

> *Remember the institutions you are talking about – the ZRP CIO and councils – do not have the technical expertise to do this. The military has, through its various specialised units like the Signals Unit which is very central to this. Again, it is a question of resources too. ZDF has money through its huge budgetary allocations, and it can afford the procurement of such cameras through its already existing relations with Chinese start-up companies like HikVision.*

HikVision is not the only player in this regard; it is, rather, a "preferred one" compared to other Chinese companies supplying the same cameras to the ZDF. For instance, the Online paper, *Biometric Update.com* (14 June 2018) reported that Dahua Technology, another Chinese surveillance camera manufacturer, would be supplying the country with video surveillance cameras on all its ports of entry and strategic public places. In addition, the global magazine, *Foreign Policy* (24 June 2018) reported:

> *The deal between CloudWalk and the Zimbabwean government will not cover just CCTV cameras. According to a report in Chinese state newspapers, smart financial systems, airport, railway, and bus station security, and a national facial database will all be part of the project – along with dozens of other cooperation agreements between Harare and Chinese technology and biotech firms.*

HikVision, however, seems to be favoured because, as Respondent 4 thinks:

> *It has close relations with the Chinese government. It therefore, can easily be included under Zimbabwe-China government bilateral trade deals, and government can guarantee its investments in Zimbabwe on the basis of these agreements.*

HikVision itself is 42% owned by the Chinese government through the Chinese Electronic Technology Company CETC Its investments in Zimbabwe, as noted by respondents, are done through the military. Respondent 2 said:

> *You should know that HikVision has invested in AI technology being championed by the military at the Zimbabwe Staff College and the Robert Mugabe Defence University. They have been there. And this surveillance technology is being rolled out into society. So, you cannot talk about surveillance in Zimbabwe without situating the military at the centre of it.*

The deals between HikVision and the government of Zimbabwe are already in the public domain. For instance, *Biometric Update.Com* (14 June 2018) reported the signing of one such agreement thus:

> *HikVision Chairman Zongnian Chen signed a memorandum of understanding with Ambassador Christopher Hatikure Mutsvangwa, who is a Special Advisor to the President, and Science and Technology Secretary for the ruling ZANU-PF party, according to a statement released by The Office of the President. President Emmerson*

Dambudzo Mnangagwa and Chinese ambassador Huang Ping were present for the signing of the agreement, under which software will be integrated with locally developed technology to drive a national facial recognition and AI system in the country and develop the local ICT sector.

The involvement of the ZDF in public space surveillance raises a number of concerns. The main questions are: Who would lead in this process to acquire facial recognition technology? The ZDF is not primarily a law enforcement entity, so why is it talking centre-stage? Where are civilian institutions constitutionally mandated with law-and-order maintenance? CSOs have also raised concerns on the usage of and post-use storage of the data.[7] How does the military intend to use the data? After use, how does it intend to store or discard the data? These questions have been contentious in the Zimbabwean context. Respondent 4 said:

The ZDF gets involved because cities and towns have become hotbeds of anti-government protests. This has elevated such kind of surveillance. Because town and city councils are controlled by the opposition MDC, we do not trust they can do this surveillance. Then you should also understand that the military is more trusted by the ruling elites [sic] than the police and the CIO. This is more so in the new system. The coup made the military more trustworthy than the police or CIO. That is why you see purges in the ZRP and the CIO post-coup. It is because there is a pervasive fear. They have been infiltrated by anti-regime elements even at command levels.

To further understand the ZDF's surveillance activities as bordering on the political, we should look at the country's crime statistics[8] available in the public domain. Urban crime in Zimbabwe is rampant in high density suburbs of the country like Mbare and Sunningdale – the Western suburbs of the capital. An explosive mixture of economic failure, agonising unemployment, absence of service delivery and general disillusionment have made these suburbs the nerve centres of crime. Yet, there are no CCTV and cameras in these suburbs. This reinforces the view that the CCTV cameras are being deployed for political surveillance.

There is yet another caveat raised by the installation of CCTV and cameras in Zimbabwe. They have widely been installed in public spaces used for political gatherings and public protests. For example, Africa Unity Square, opposite the Parliament of Zimbabwe, is a well-known place for opposition gatherings. As a report noted, (*NewsDay*, 2018), there was no due consideration of the constitutionality of such a move, neither was there consultation with the public or city authorities. More so, in the broader picture, CCTV and cameras have always been controversial. Their effectiveness as crime-fighting devices (Moon, Heo, Lee, Leem & Nam, 2015) has long been questioned. But others have argued that, if fully functional, CCTV and cameras can be effective in fighting crime, or, at least have the potential to do so (Moon et al., 2015). There is recent evidence, however, to the effect that CCTV and other cameras do not fight crime, they merely displace it (Waples, Gill & Fischer, 2019).

7 See Rights to Privacy periodic review: http://hrp.law.harvard.edu/wp-content/uploads/2016/04/zimbabwe_upr2016.pdf.

8 See crime statistics here: https://www.numbeo.com/crime/country_result.jsp?country=Zimbabwe.

The ZDF's communication surveillance capabilities

The ZDF, according to respondents, has an (ever) growing capacity for cyber-communication surveillance. Respondents noted that this capacity lies particularly in: (a) IMSI catchers that operate as cell phone towers, allowing the user to track particular cell phone signals; (b) a variety of spy phone software; (c) software programs that monitor personal computers and allow for "deep packet inspection"; and (d) email snooping software. Credible news sources and interviewees identify Iran as the major supplier of these technologies. The *Telescope* newspaper, for example, reported on 26 January 2015, that:

> *The Islamic Republic of Iran has granted as a gift to Zimbabwean leader, President Robert Mugabe's regime, a dreaded cocktail of cyber and surveillance technology. The cyber technology, which includes among other things: Spy-phone software; IMSI catchers; another program to monitor personal computers, will soon be tested at the Zimbabwe Defence College.*

Foreign Policy (24 July 2018) noted the same and reported this:

> *Tehran has been making efforts to help Zimbabwe snoop on the information superhighway, a move that has shocked Zimbabwe's human rights activists... Through a technique called "deep packet inspection", Iran's sophisticated mechanisms of controlling the internet enables government authorities to not only block communication but to monitor it, to gather information about individuals, as well as alter it for propaganda purposes...which is a dream, come true for Mugabe's egregious security law.*

To fully exploit the acquired equipment, the ZDF has, in the years since 2015, or even before, held joint training exercises with the Islamic Republic of Iran military on how to make use of these technologies. However, we need to equally acknowledge that deep packet inspection has legitimate uses, like "sniffing out" network intruders meant to steal people's data. But this does not of course preclude the likelihood that in Zimbabwe's semi-authoritarian context there are rogue uses of DPI, like monitoring of citizens.

What is disputable, though, is whether the acquisition of cyber-communication surveillance technologies by the ZDF started around 2015. The broad agreement from respondents is that it started much earlier. Respondent 3 said the capability of the ZDF in this regard was acquired over a decade ago:

> *This capability was there for some time. I cannot pinpoint a specific time period, but if you go back and check on events, you will realise that the ZDF was already snooping on private emails a long time back.*

As Respondent 3 noted, there is, indeed evidence that as early as 2005, the ZDF was already snooping on private email. One notable example is that of Elizabeth Macheka-Tsvangirai, the wife of Zimbabwe's former Prime Minister and opposition leader, Morgan Tsvangirai. In August 2013, her private email correspondence with an alleged lover was splashed in the state-owned but ZANU-PF-controlled public newspaper, *The Sunday Mail*. Zimbabwe Lawyers for Human Rights (ZLHR), the Crisis Coalition of Zimbabwe (CCZ) and other organisations, including the opposition party the MDC, all pointed to the state security institutions as responsible for snooping on Tsvangirai's wife's emails. The newspaper itself was mum on where it got the emails, but one thing stands out for certain – the paper had no capacity to snoop into private emails, and there was consensus that it was the state, with both the capacity and intention to ruin Tsvangirai's standing.

What was lacking in this particular incident, was a broad consensus as to which of the three state security institutions was involved – the ZRP, CIO or ZDF? There are contradictory accounts of what transpired.

Some elements within the opposition think that the CIO that was responsible for snooping into peoples' emails. Those who hold this view go on to allege that the CIO is assisted by malleable MNOS and ISPs who allow them access to their internet traffic. *The Independent* newspaper of Zimbabwe presented this view. On 6 September it wrote:

> *... Snooping fears come as state security has stepped up mass surveillance on private citizens, particularly those perceived as political threats, as the monitoring has widened beyond phone-tapping and e-mail interceptions to scrutinising activities on social media such as Facebook, Twitter and WhatsApp. Targeted groups and individuals' communication activities are being monitored by the much-feared Central Intelligence Organisation (CIO) from designated listening posts in Harare, mainly in Mount Pleasant.*

The newspaper quoted a government insider as saying,

> *The CIO obtains recordings of voice calls and other material from local cell phone providers under the guise of carrying out state security operations.*

Another view, corroborated by interviewees, is that it was the ZDF's Signals Unit, well able to carry out such sophisticated cyber-communication surveillance as establishing listening posts, that was snooping on emails. Respondent 6 noted:

> *The ZDF's Signals Unit is well-equipped for this. All the other institutions would have to seek its assistance. It can even bully MNOs and ISPs to provide whatever information they may want if need be. But it's even rare; they get their own information via their own technologies.*

In Zimbabwe's conflated institutional arrangements, it is indeed true that the ZDF's qualified personnel are often called upon by other institutions when their expertise is required (MPDP, 2019). Respondent 7 stated:

> *The ZDF's staff college is the one fully equipped for this. Make no mistake, it is them. And they have targets they want. But they are still accumulating such technology to broaden their activities, and to do it at larger national scale [sic], and of course to keep up to date with new technology.*

The more recent Job Sikhala case lends credence to respondents' claims. Job Sikhala is one of the Vice Presidents of the opposition MDC Alliance. On 10 August 2020, the ZDF descended on the Dema rural area, just outside of the capital Harare, in a door-to-door search for the MDC-Alliance Vice President. He was wanted in connection with charges of attempting to overthrow the Mnangagwa regime. The question was, how did they know he was hiding in that area? Jonathan Moyo, a former cabinet minister, and close ally of Robert Mugabe, knew the answer, and tweeted:

> *They are looking of him with a vengeance in a door-to-door operation, after picking up his phone signal!!*

One cannot dismiss this tweet lightly, considering that Moyo was a cabinet minister and very close to Mugabe in the system for more than 10 years; he might well know of this capability considering his long stint in cabinet and his role as Mugabe's Minister of Information.

The ZDF's cyber-communication capabilities, just like its public space surveillance practices, raise many questions. Under Zimbabwe's Defence Act, (Chapter 11/02), the ZDF is a

"national defence force". The crime-fighting capabilities of the ZDF are constitutionally limited to state emergencies. Under such circumstances, the President of the Republic may deploy them for a period of six months to assist the ZRP in fighting crime and restoring order. Any further extension would require permission from the country's National Assembly. This means that the current activities are politically motivated, as there is no declared emergency, neither is there parliamentary sanction.

Enablers of ZDF's surveillance capabilities

This section answers the question: Who are the funders enabling the growth of ZDF's digital surveillance capabilities? This research shows the existence of an assorted mixture of global organisations largely helping with the acquisition of the ZDF's surveillance resources. These global enablers can be ranked in their order of importance – that is according to the "size" of their assistance to the ZDF's ambition. If ranked in this order, they are: the Chinese government; Chinese-based technology companies; Iran and Russia.

The government of China has been the most consistent and frequent enabler in this regard. It has helped its Zimbabwe counterpart in two major ways. First, the Chinese ruling regime has provided loans and grants on very favourable terms. In turn, the Zimbabwe government has appropriated these loans and grants to the ZDF to enable it to directly purchase surveillance technology from manufacturers largely based in China. The cheap loans have come at a time when the Zimbabwe government has been deprived of such by Western governments since the controversial land reform programme in the early 2000s (Tendi, 2019). Secondly, the Chinese government has also supplied spy technologies directly to Zimbabwe. In both ways, it has boosted the surveillance capabilities of the ZDF. Respondent 6 remarked:

> *There is a growing relationship with China which the ZDF has benefitted from … this is in addition to what you already know … combat weapons.*

The point was corroborated by MISA (2018), which declared:

> *China, Iran and Russia are helping the Zimbabwean government to set up a security arm or body with surveillance capabilities similar to those of the United States' Central Intelligence Agency and the National Security Agency. Facial recognition technology would also work well with the smart cities' initiative, which was launched in Harare in mid-March, an initiative which the government backed.*

The state-controlled mainstream daily newspaper, *The Herald* (2019, n.p.), largely seen as the mouthpiece of the ruling elite, confirmed Chinese involvement, citing the former Zimbabwe ambassador to China, Chris Mutsvangwa saying, "… Zimbabwe [the ZDF in particular], has recently received donations of facial recognition terminals from CloudWalk tech, a company based in South China's Guangdong province…" In another such confirmation, the weekly state-owned mainstream newspaper acknowledged that China had donated a drone which is now part of the president's security. The admission was made after numerous private news platforms had reported a drone sighting during the president's visit to the Midlands province. This confirms how surveillance technology has been deployed to many other uses within the ZDF. An interviewee, Respondent 7, confirmed this:

> *China has donated a number of drones and other spy techs to this country. Sometimes if the equipment does not serve [military] intentions, it is passed on to relevant departments … because these are donations, you can redeploy them.*

Respondent 5 recalls one of these donations, disclosing:

> *At one point we passed two surveillance drones to the Ministry of Wildlife because they had equipment that suited their particular ministry...*

The donation was further confirmed by *The Herald*, which reported:

> *The ZNA has donated a two-seater microlight aircraft that will hover in the sky providing surveillance in the 2 196 square kilometre Mana Pools National Park.... The aircraft was sourced from China.*

There are five Chinese technology companies noted as being very active in providing spy tech equipment to Zimbabwe. These are: Huawei, ZTE, CloudWalk, Hikvision and Semptian. These are by no means the only ones, as many Chinese start-ups were also engaged with the Zimbabwe military in the purchase and supply of spy technology.

Thus, the ZDF has struck a continuous relationship with an assorted mixture of players in the supply of digital surveillance technology. The ZDF's choice of suppliers is, by default, influenced by a number of factors. Chief amongst these has been the country's inability to access Western markets for these technologies due to Western-imposed sanctions that prohibit Western countries from trading with Zimbabwe in this and other security-related equipment. But, beyond this reason, the country's choice of surveillance technology suppliers is, arguably, shaped by two more political considerations. First, Zimbabwe's main suppliers willingly supply these technologies of surveillance regardless of the buyer's human rights history. This is evident from the fact that despite Zimbabwe's parlous human rights record that has often brought global censure, no company from these countries has stopped the trade in surveillance equipment. Second, these suppliers would not mind whether their clients declare the end-users of their technologies. This may not be the case with most Western technology companies, who might be concerned about these considerations, especially when the country concerned is under Western government sanctions as is the case with Zimbabwe. Because Zimbabwe's suppliers are not likely to ask human rights questions (see *NewsDay*, 2020), it means their surveillance technologies can be used for cracking down on political dissent, which is the case in Zimbabwe.

The political economy of surveillance: The actors and interests within ZNA

The actors

The next important questions to ask was: who are the actors within the military intrinsically linked to surveillance practices, and what are their interests? There are specific entities within the military that are responsible for surveillance, according to reports and interviewees. Thus, the whole entity is not tasked with surveillance for three major reasons. First, it is simply hopeless to equip the whole ZDF with both the equipment and technical know-how of the practice.

Zimbabwe, as a country, may not be able to afford the costs of such a grandiose endeavour. Second, if surveillance is spread across the whole military, it ceases to be secretive and effective. Third, the interviewees disclosed that the majority of the army and its commanders are actually internal targets of surveillance themselves. Respondents noted that factionalism within the ZDF has been a serious concern for the ruling elite, together with other intervening factors, like increasing cases of indiscipline and desertion, such that members of the force and other security agencies have themselves become targets of surveillance. Rupiya (2011), has proved in many instances that the ZNA is a politically factionalised entity. The political factionalisation of the ZNA dates back to around the 1980s, and erupted in violent confrontations in some instances (Hawkins, 1981). These factional cleavages have always pitted senior commanders against junior army officers (Maringira, 2017), who have resisted the "Zanufication" of the military. However, while the existence of factions in the military is known, it is not yet clear which units align with the sitting President, and which ones align with his Vice President, Chiwenga. Yet, as Respondent 3 noted, "There is now surveillance and counter-surveillance within the military ... heightened by increasing factionalism, but who reports to who is not clear, from at least what I knew..."

What has happened in the post-coup period is an intensification of this factionalism. The factional fragmentation of the army under Mnangagwa has intensified because, [he lacks] …adroit skills [like Mugabe]… and hence the sense of rudderlessness and incoherence in the party…" and the state's institutions in general (Hove, 2019, p. 67). At present, reports (*The Zimbabwe Independent*, 2018), point to the existence of a factional group opposed to the current President, generally in favour of his deputy, Constantine Chiwenga, to take over power. Respondent 3 commented:

> *These factions are thought to exist within the army. And these has [sic] exerted real terrors among the leaders … you can see they are concerned by the behaviour of the commanders … and if you are clever you would not do suspicious things … I think by now most soldiers know they are surveilled, especially if you have a commanding position.*

But then, which entities are responsible for both internal surveillance (within the army itself) and for civilian surveillance? Respondent 5 noted:

> *Digital surveillance is a preserve of three departments in the ZNA. These are the Signals Unit (SU), the Zimbabwe Intelligence Corps (MI) and the Special Intelligence Branch (SIB).*

The SIB normally investigates indiscipline within the military. Respondent 2 stated, however, that this was no longer the case. Its practices have widened away from being focused on internal indiscipline within the military to being used for non-military surveillance. Thus, the unit has become useful in the whole civilian surveillance architecture of the ZDF.

The Zimbabwe Independent (2018) confirmed that specialised units of the ZNA like the Special Air Services (SAS), a specialised branch of the ZNA based at Kabrit military base in the capital Harare, also undertakes digital surveillance. Respondent 8 concurred with this report, remarking:

> *These units like SAS Commandos are highly skilled and they can do everything. It is not surprising that they are part of covert surveillance. After all, they are also major recipients of modern-day spy and military tech from China and other countries.*

The SAS is a highly specialised branch of the ZDF. It specialises in different types of warfare, search and destroy missions, weaponry use and

many other skills of war. It is also highly equipped and works with both the army and the air force, according to respondents.

The interests

Respondents noted that the interests of military-driven surveillance are not cast in stone. They mutate over time to meet the current economic, political and social conditions obtaining in Zimbabwe at a particular time. However, respondents noted that the major interest was, broadly, political – to keep the regime in power by destroying any threats to its power. In line with this broad interest (see the next section on targets for furtherance of this argument), Respondent 4 declared:

> *The major purpose of surveillance is to predict civil unrest induced by the opposition party/ parties by collating data on opposition leaders, and other sources of unrest and pre-empt them through, for example, arrests … and disrupting their plans.*

Within the military itself, surveillance is meant to:

> *Track violent dissent against the regime, including dissent in other security agencies like the CIO and the ZRP (Respondent 1).*

Why has the military become a target of its own surveillance? Respondent 4 suggested:

> *The economic conditions in the country can trigger a lot of indiscipline in the armed forces. Already the army is struggling with desertions … absenteeism, and there is fear of a possible military mutiny according to The Independent (24 August 2018).*

This fear is not far-fetched. In 2000, *The Zimbabwe Standard* newspaper reported that ZNA soldiers deployed in the Democratic Republic of the Congo had mutinied. Therefore, the ruling elite's fear of a mutiny is real. Then there is also the question of loyalty. It is still not certain, according to Respondent 5, if all members of the ZDF are loyal to the new regime.

Hence, digital surveillance targets potential nodes of revolt within the force that might destabilise the government. Respondent 2 added:

> *There has never been one hundred percent trust with [within?] the force, even during the Mugabe period … The economic decline of the post-coup period has worsened the situation. I tell you, there are strong sentiments within the military forces that Mugabe was an angel … the elites [sic] are very much aware of this disillusionment … and the soldiers are also aware that they are under possible surveillance.*

Evidently, the main interests of surveillance are to maintain a "panopticon grip" on the military, which since the year 2000 has become an arbiter of Zimbabwe's politics (Rupiya, 2016). As the Zimbabwe military become increasingly factionalised and politicised (Maringira, 2017), the ruling party is determined to maintain a tight grip on this (political) power-conferring institution. The process of ensuring blanket surveillance on the military (and even on the civilian population), however, is threatened by a deteriorating economy which has dried up patronage resources that have been distributed to the force to buy their loyalty (Maringira, 2017). The obvious danger is that if the military cannot enjoy the wealth and comforts of the economy, a full-scale violent implosion may be difficult to forestall in the long run.

The Independent report (2018) further points out that rising tensions within the ZNA, wrought by inflation and basic commodities shortages,

have led to "… growing discontentment among troops. Reports from the directorate show that morale has hit rock bottom … this has triggered the deployment of surveillance within the rank and file of the military." The report further notes, "The internal surveillance, being undertaken by the MI and the military police, has been necessitated by growing disquiet within the rank and file of the military over the rising cost of living, poor salaries and difficult working conditions."

Surveillance therefore serves the interests of the ruling elite to stamp on disquiet within the force, and it is, by and large, motivated by this fear of mutiny.

It was also noted that, within the security branches of the state, surveillance was also targeted at the police and the CIO. According to respondents, these branches have been viewed as very much pro-Mugabe. Tendi, (2019) has also confirmed that during the coup, the army had to neutralise the police and the CIO as they were viewed as pro-Mugabe. Respondent 4 said:

> *If you were following the coup, the police support unity base at Tomlinson was surrounded by the military, and senior CIO officers were also taken into custody. These institutions and their top elites were not trusted as allegiant to the new people … and they have been under military surveillance for a long time before the coup.*

In a country like Zimbabwe that publicly claims to be democratic, military-driven surveillance of civilians stands in stark contrast to the democratic ideals purportedly upheld by the regime. Furthermore, on top of consolidating a "digital authoritarianism", surveillance raises a number of questions. For a start, to whom is the military's covert surveillance practices and data collection that comes with it, accountable? This is crucial to think about, considering the fact that the ZDF, outside of an emergency, has no crime-fighting powers. Therefore, it should not delve into surveillance practices involving civilians. Their illegal involvement in this raises further questions: What happens to the data they gather? How will it be stored? What guarantees are there that it is not sold, for commercial purposes, to third parties? None of these questions can be answered sufficiently in the Zimbabwean case because in the first place, military-led surveillance is a mission creep with no legal basis.

Global standards of surveillance[9] have devolved two very important mechanisms around surveillance. First, post-surveillance notification is important in digital surveillance practices. This practice ensures that, as a right, targets of surveillance are informed post-facto. Second, both judicial authorisation and oversight have become key pillars of surveillance practices in the post-Snowden period. In the Zimbabwean case, these two crucial elements are missing. This confirms that surveillance in the country is a political, not crime-fighting, practice. Thus, one can argue that post-coup Zimbabwe has become one side of the same coin with the Mugabe regime. The difference, based on the evidence, might be that post-coup Zimbabwe has witnessed hardening digital authoritarianism driven by the military, compared to the Mugabe period. Outside the military itself, who else are the targets of military driven surveillance?

External targets of military-driven digital surveillance in Zimbabwe

There are four categories of external targets of surveillance outside the ZDF, which will be fleshed out in this section. By external targets, I use the word to mean targets outside the structures of the ZDF and other security organs of the state. These four are: (1) senior opposition party members, especially those aligned to popular opposition leader Nelson Chamisa; (2) civil society leaders

9 The United Nations Human Rights Office. www.ohchr.org.

and USAID-aligned NGOs; (3) senior ZANU-PF members, and (4) ordinary citizens who use social media for political expression, regardless of political affiliation.

The Zimbabwean regime has always pushed a narrative that "demonises" CSOs and NGOs as "regime change agents". Based on this narrative, state security agencies have treated these organisations as such – as organisations bent on helping the opposition parties to power. As such, operational restrictions[10] have been instituted on these NGOs and CSOs. These have been worse in instances where these entities' funding has a direct link to USAID, the EU and the DFID in particular. These organisations have always been accused of harbouring a regime-change agenda in Zimbabwe, meant to depose ZANU-PF from power (see Sachikonye, 2012). Respondent 6 notes:

> *What I know is that the authorities have tasked not only the military, even the CIO and police intelligence units like PISI, to surveil on the leaders of CSOs and NGOs. These have always been thought to work in cahoots with the opposition … so their activities are suspicious and should be monitored.*

Respondent 5 agreed, adding:

> *There are high priority CSOs and their leaders. These are organisations in the field of human rights, democracy and elections. These are on the top of the surveillance list and any other surveillance. When we know how they operate, we can shame them. We can also destabilise them.*

Snooping on CSOs also extends to the leaders of these entities. This was confirmed by Respondent 4, who noted:

> *Surveillance targets also include leaders of these organisations. They have to be monitored and their activities noted. Anything and anyone with a link, no matter how remote, to Western sources of funding, is a suspect.*

A report[11] confirmed the active role of the military in the surveillance of CSOs and NGO, noting thus:

> *The Zimbabwe National Army's Military Intelligence (MI) unit has placed on its watchlist several civil society activists it claimed were conniving with United States to unseat President Emmerson Mnangagwa through violent activities...*

The *Zimbabwe Independent* investigative unit further revealed:

> *The MI is a military unit that uses information collection and analysis to provide guidance and direction to assist commanders in their decisions. In a recently circulated internal memorandum seen by the Independent this week, the MI claims it has gathered intelligence on people, who it claims are being sponsored by and working closely with US nationals to unleash a wave of attacks "on strategic points using small arms, homemade bombs and explosives". The targeted individuals, however, dismissed the allegations saying they are MI fabrications targeting the MDC and labour organisations who threatened to roll out demonstrations.*

Opposition leaders have also been the major targets of surveillance practices by the military. The opposition MDC has been a major threat to ZANU-PF's hold on power. This threat has worsened since the disputed 2018 elections and the subsequent post-election violence that

10 Zim NGO Bill restricts operations: https://reliefweb.int/report/zimbabwe/zimbabwe-ngo-bill-likely-restrict-human-rights-operations.

11 *The Zimbabwe Independent* (14 June 2019). Civil society leaders on military watch list. https://www.theindependent.co.zw/2019/06/14/civil-society-activists-on-military-watch-list/.

erupted. Interview sources noted that there are two considerations that inform the surveillance on opposition leaders. Respondent 6 said:

The fear in the regime is that these opposition leaders can align with the remnants of the G40[12] to form a potent combination that can threaten their hold on power. The other consideration is the fact that the opposition, especially Chamisa, has urban support; he can lead a spontaneous revolt you know … and the conditions on the ground support one.

These two considerations have prompted the military to prioritise surveillance of leading opposition figures. Surveillance of opposition leaders and outspoken critics of the ruling party might have intensified in the post-coup period, but the practice is not peculiar to this period alone. For instance, the late opposition leader, Morgan Tsvangirai's wife Elizabeth Macheka's emails were "leaked" to the media and her conversations eavesdropped and leaked too, in a move where CSOs pointed at the military[13] for possessing the necessary technology. The emails, about Macheka's alleged extra-marital affair with Kenny Ngirazi, were widely covered by the state-controlled press – especially *The Sunday Mail* and *The Herald*. CSOs and interested individuals were left wondering who else possessed such surveillance technology to remotely tap conversations and snoop into emails. Fingers of scorn were pointed at the military, which, in around 2012, had received IMSI catchers and its personnel trained in Iran.

In July 2007, suspected military personnel planted a video recorder in the house of one of Mugabe's fiercest critics, Archbishop Pius Ncube. He was caught on camera in "an adulterous relationship with a married woman…".[14] The leak led to his defrocking, and eventually silenced him. Two weeks before the leak, Mugabe had hinted at it, which shows that the leak might have been the work of the state, and organised at an elite level. Mugabe specifically said, "Some of them [clergy] claim they swore to celibacy, yet they sleep around with countless women" (*The Telescope* 12 September 2015). These incidents have not gone unnoticed as proof of state involvement in surveillance, especially of its critics.

In the post-coup period, senior ZANU-PF members have not been spared from surveillance, according to sources. The reason has been their allegiance. The ruling elite, according to interviewees, are not sure if the senior party members owe their allegiance to the current top five of the party. Respondent 6 noted:

> *There are several officials who are targets of surveillance by the army. Their association with Mugabe leaves their allegiance suspicious. And the ruling elites [sic] is aware that some jumped ship on the last minute.*

Respondent 8 concurred:

> *The fear is that they might still be in touch with the now vanquished G40 faction of the ruling party … their association has to be monitored … they also have to be monitored themselves.*

But how serious is surveillance of ZANU-PF officials compared to opposition officials? Respondent 5 replied:

> *In my view, both are viewed and surveilled equally. For the opposition the failed demonstrations that characterised the country after elections, and the January 2019 demonstrations were enough to strengthen the case of their surveillance. I know there was a time when military intelligence was asked to prioritise the opposition leaders … it was because they were a real threat.*

12 The G40 was a ZANU-PF outfit that backed Mugabe and fought against the rise of Emmerson Mnangagwa to the presidency.

13 Zimbabwe Coalition for Human Rights Report: https://cutt.ly/rjGg4gA.

14 For the story follow: https://www.theguardian.com/world/2007/jul/21/zimbabwe.chrismcgreal.

Respondent 5 further noted:

> *I also remember there was a time when there were serious leaks of state secrets and ZANU-PF politburo meetings. The surveillance branches of the military were on high alert about this. The suspicion was that there were people in power who were responsible.*

Move towards dragnet surveillance? Some reflections

From the evidence provided by respondents and reports analysed here, it is evident that the ZDF is practising surveillance, and simultaneously building surveillance capabilities. At this stage, it is too early to say the ZDF has achieved a panopticon-like dragnet digital surveillance on the country. But if one reflects on the evidence presented here, there is little doubt that the ZDF has such intentions.

There are key signs and motives why the ZDF might want to achieve a dragnet-type of surveillance for the whole country. Firstly, as evidence has shown, the ZDF is already exploiting its agreements and the government's own agreements with Chinese technological companies and the Chinese government itself, Russians and Iranians, to acquire surveillance technology. As long as these agreements are in place, it means the accumulation may continue unabated. Secondly, opposition to the current political status quo is growing, hence providing a *raison d'être* for the continuation and broadening of current surveillance practices beyond the current targets. Thirdly, the ZDF enjoys a relatively huge budgetary allocation from the national treasury. This means it can afford its own purchases in addition to loans and grants provided by the Chinese. Fourthly, there is very little CSO activism and media awareness in the country around these issues, which means the ZDF's build-up of surveillance capabilities may, at least in the short term, likely meet with little to no resistance in the form of, for example, litigation.

MISA-Zimbabwe has been doing appreciable work conscientising the public about the growing danger of growing digital surveillance. But this looks like a "lone-wolf" battle on behalf of a disinterested public, seemingly fixated on survival in a rapidly deteriorating economic environment. In any case, the ruling party elite have always viewed alternative views as Western-sponsored. So, even the activism is likely to achieve little. But too little is still a positive starting point compared to none at all.

The military's own public pronouncements indicate that it seeks to achieve total surveillance especially of social media platforms. This means that ordinary Zimbabweans on social media would be watched by big brother, in typical panopticon style. It was reported in 2019,[15] that, the ZDF, "…would soon start snooping into private communications between private citizens to 'guard against subversion'," alarming media groups who feared that the country was moving towards a surveillance State.

Considering that many Zimbabweans use these platforms, it is a tell-tale sign that the ZDF has intentions of dragnet surveillance.

The Commander of the ZNA has specifically said:

> As commander of the Zimbabwe National Army, I am happy that the course laid a proper foundation in the areas of cyber security, which pose a dangerous threat to our national security … Social media poses a dangerous threat to our national security … one of the tools that is being used for misinformation and I believe that your training has been an eye-opener to the rigours and realities of technological advancements … that we must deal with immediately. (*NewsDay*, 23 March 2020).

15 *News Day*: https://www.thezimbabwemail.com/main/zimbabwe-military-to-snoop-on-social-media/.

There are two major factors that might halt a speedy move towards blanket surveillance:

1. Dissent within the ruling party elite, as some realise, they can be targeted for surveillance, might hopefully stall the ZDF's surveillance build-up, as these members of the elite may not want to pass the decisions enabling this.
2. The current economic implosion may mean that the ZDF cannot afford the foreign currency required for sustainable purchases. Already, the government is defaulting on payments on some of these loans.[16]

But, basically, the ZDF's ambitions are clear, though there are many stumbling blocks towards that goal.

16 Zimbabwe defaults in Chinese loans: https://www.thenational.ae/business/culture-of-default-has-hurt-zimbabwe-s-credibility-1.164358.

Concluding remarks

This research sought to explore military-driven surveillance practices in Zimbabwe. It has found that the involvement of the military in digital surveillance is growing. This has been boosted by technical and financial capacity being provided by cooperating global partners like China, Russia, Iran, and Chinese start-up companies. Surveillance has largely been used for political rather than crime-fighting purposes. The involvement of the military comes at a time when there is no clear legal mandate for them to carry out surveillance practices. The major problem, however, is that Zimbabwe's surveillance legislation, particularly the Interception of Communications Act, is seriously flawed. This has allowed the military to practice surveillance without a clear legal mandate. The practice, traceable to the Mugabe period, has gained momentum in the post-Mugabe period. There are many issues in this field that still need examination. For instance, how are CSOs, individual citizens and targeted constituencies like opposition members and journalists responding to surveillance? What kind of resistance are they mobilising? Every kind of digital surveillance has been known to generate resistance efforts by targeted groups, no matter how weak or futile these efforts might be (Fernandez & Huey, 2009).

There is also need to explore, in detail, the political economy of surveillance in the country as an independent area of research. The strength of this research project lies in the fact that it has mapped the terrain in detail; further research is not only possible, but necessary, in order to have a clear understanding of this developing practice in the country. Researchers in this field should take advantage of the opening provided by the rift within Zimbabwe's institutions as a result of post-coup power dynamics. Important constituencies might be willing to open up, and important information may be obtained. There are still gaps in research, though, that need to be filled in the Zimbabwean context. For instance, this research could not explore the following key areas, and I recommend that they be tackled to provide a clear picture on digital surveillance in Zimbabwe:

- Resistance to military-driven surveillance – the capacity of civil society organisations (CSOs) in driving the resistance agenda to surveillance
- Legislative provisions and oversight mechanisms on surveillance, and their adequacy in protecting people from unauthorised surveillance.

Key policy recommendations

Several recommendations can be suggested, based on the findings made in this report. These recommendations have been made for the following constituencies: (i) the Government; (ii) CSOs; (iii) the media in Zimbabwe; (iv) the ZDF; (v) the National Assembly of Zimbabwe, (vi) opposition political parties; and (vii) the ruling party, ZANU-PF.

These recommendations are meant to make surveillance practices legal, transparent and non-military.

The Government of Zimbabwe

There is a need to prioritise the ICA as a matter of urgency, so that it is in line with international standards of surveillance. In the process of revising the law, government should consult all stakeholders. The Minister responsible for communication and technology in the current government, should drive reforms of the ICA that should target the following aspects:

- Ensure the adequacy of measures that grant judicial authorisation and oversight in the surveillance process. The current procedures are both deeply flawed and inadequate, as they are more executive than judicial.
- Post-surveillance notification should be added into the law. The current law does not provide for it, which is a serious flaw. Post-surveillance notification provides that a subject of surveillance should be notified that they have been subject to surveillance
- The role of security agencies like the ZRP and the CIO should be clarified in the constitutional amendments. In the same vein, the ZDF should desist from civilian surveillance. Their capabilities should be focused on external threats to the country, and if and when called upon by other state security agencies, especially in crimes that threaten national security. The current situation outlined in this research is illegal.
- Ministerial powers should be watered down, and surveillance authorisation should be transferred to competent judicial authorities, bearing in mind that the minister is a political appointee.
- The amendments should adequately deal with data protection so that it is clear what happens to (meta) data post-surveillance. The deposition of data should be in line with international standards.

Civil society organisations

Although the space for participation and consultations has been drastically limited due to draconian legislation by the state, CSOs should use that limited space available to them to engage the regime on cyberspace legislation broadly, and surveillance in particular. From my observation, CSOs seem to have surrendered to the belief that they are powerless to influence and shape laws on surveillance due to the proven non-consultative approaches of the ruling class. But I recommend that CSOs start utilising the small window of opportunity available to them to achieve the following:

- Work actively with other players in the field, like human rights activists, lawyers, academics and technology specialists, to make inputs in

the legal and policy processes around digital surveillance

- Take part in broadly constituted forums that discuss the issue of digital surveillance in the country
- Involve themselves in drafting policy briefs and position papers on digital surveillance, and help through, for instance, mobilising the media, in conscientising the people about the need for transparent and independent surveillance legislation frameworks
- Vigorously engage the Parliamentary Portfolio on Communication Technology, which handles cyberspace law legislations.

The media in Zimbabwe

Conscious of their role as the fourth estate, the media is encouraged to start setting a public agenda on the illegal military-driven surveillance currently being practised by the Zimbabwean authorities. The media's role and attitude in this regard is, currently, peripheral and lukewarm. There are encouraging signs, however, that some journalists have started writing[17] about military-driven surveillance in the country and how illegitimate it is. What is needed is to sustain this narrative and ensure it reaches as wide an audience as it can. I have noticed that the subject of surveillance is treated in Zimbabwe as if it is an elite issue. The media should be the voice articulating this practice in simplified ways for the audience. In this vein, I point to two very important processes that will strengthen the media in reporting digital surveillance:

(1) *Capacity building*: Media organisations in Zimbabwe like the Zimbabwe Union of Journalists (ZUJ) should help address the capacity gap through training so that journalists have knowledge of surveillance issues beyond rudimentary know-how. Journalists should also be trained to understand international best practice in digital surveillance, and legislative practices around digital surveillance both within and outside Zimbabwe. This would help journalists sustain a discourse on the subject in a way that informs the community.

(2) *Regional and global synergies:* Zimbabwe journalists should start working with organisations that focus on digital surveillance at a local and regional level. This would help them to keep abreast of the issue and report in an informed manner. This will also help them shed light on and point out problematic legislation and processes pertaining to surveillance in their own (Zimbabwean) context.

The Zimbabwe Defence Force

The ZDF should be reminded that the Zimbabwe Defence Act (Chapter 11/02) does not give them permission to practice the surveillance of civilians outside the constitutional framework and provisions, as is the current situation. They should be reminded that their current practice lies within the purview of the ZRP and the CIO. They should, therefore, be mindful of their role as enshrined in the constitution. Above all, they are a national defence force, not a (ruling) party militia. The current practice turns their behaviour into that of a party militia. They should, hence, leave this responsibility to the agencies with this constitutional mandate. The commanders of the ZDF should be aware that military-driven surveillance crosses a constitutional line that can possibly lead the country onto a path of digital authoritarianism from which it might not return. The constitution makes it clear under the Defence Act and the Presidential Powers and Temporary Measures Act (Chapter 10:20): the military can engage in such practices during a state of emergency as defined by the President, and during a war or any other armed insurrection against the Republic. There is no known emergency

17 See Dumisani Dhlela's news report "Military surveillance endangers democracy" on: https://www.newsday.co.zw/2020/03/military-surveillance-could-endanger-democracy/

declared in Zimbabwe. And there is no known war or armed insurrection the ZDF is involved in. Hence, the current practices are unconstitutional and unacceptable in a country purporting to be a democracy.

The involvement of the military in civilian digital surveillance practices outside a war or other periods of armed insurrection impinges on democratic norms and values and has many negative ramifications for individual privacy. This is even more so in semi-authoritarian contexts like Zimbabwe.

The ever-growing role of the military in civilian digital surveillance means military domination in matters that are largely civilian. This eclipses the constitutional roles of the ZRP and the CIO. Because the involvement of the military is only permissible during armed conflict, in which they are involved, their current involvement is anti-democratic, considering that Zimbabwe claims to believe in strict adherence to the rule of law and constitutional order, hallmarks of democratic states (Ottaway 2013). This, therefore, constitutes a "mission creep" that upsets the power dynamics of institutions provided for by the constitution – where roles are "fenced off" to avoid the encroachment of one institution of the state into the role of another institution.

This is a serious threat to democracy's principle of political opposition. And it's even a worse threat in the Zimbabwean context where the military is a well-documented partisan institution (Sachikonye 2011; Masungure 2020). Under these political circumstances, military-driven surveillance would fortify authoritarian tenets of the regime. A lasting consequence would be the creation of a docile population, cowed and seduced into political submission to the ruling regime due to lingering fear of unconstitutional military-driven surveillance. Lastly, it is against international best practice of surveillance for the, military surveillance ideology to (dangerously) into civic realms.

The National Assembly of Zimbabwe

The legislative body should immediately lobby the Minister for Information and Technology to lead the process of amending the ICA and all related instruments to ensure that they are in line with international standards and Zimbabwe's regional and international treaty obligations. It is important that the National Assembly speed up this process and tap into existing academic and professional expertise on the subject that the Assembly itself may not have.

Opposition political parties

Zimbabwe's opposition parties should be active in pushing for the amendment of the ICA. They should do this privy to the fact that they have broadly been amongst the central targets of military-driven surveillance in the country. It is important for them to wrest the agenda away from the ruling party elite who may not be very interested in changing the law, which, at the moment, is still serving them. But the opposition should be part of this process. Currently, there is no evidence that the opposition has a view on the issue of ubiquitous military-driven surveillance. Surveillance has hurt free and fair elections which have been a central dispute in Zimbabwe's politics. If opposition parties turn a blind eye to these developments, the region will remain saddled with disputed elections in the country and this means the central definer of the "Zimbabwe crisis" will not go away.

The ruling party, ZANU-PF

The ruling party legislators should stop abusing their parliamentary majority by passing surveillance legislation that does not meet globally accepted standards. If the ruling party is serious that the current regime is "a new dispensation" as it claims, it should push back against Mugabe-style legislation like the Cyberspace Bill currently before parliament. The bill still falls far below

acceptable standards. For instance, it still lacks judicial authorisation of surveillance. It is still not clear in the bill what happens to the data post-surveillance, and above all, there is no provision for post-surveillance notification. This opens up room for abuse, where the ZDF may creep in unchecked by legislation. Therefore, ZANU-PF should pause such draconian legislation, consult with CSOs, NGOs, the opposition, and all interested parties in this bill. Otherwise, the much-talked about ZANU-PF-led "new dispensation" may remain a myth, or a "new desperation".

References

Barkan, J. (2005). Emerging legislature or rubber stamp? The South African National Assembly after ten years of democracy. Available from: https://open.uct.ac.za/handle/11427/19368

Biometric Update.com (2018). Zimbabwe to use HikVision facial recognition technology for border control. Available from: https://www.biometricupdate.com/201806/zimbabwe-to-use-hikvision-facial-recognition-technology-for-border-control

Calatayud, M.M. & Vázquez, A.S. (2018). Mobilisation and surveillance on social media: The ambivalent case of the anti-austerity protests in Spain (2011–2014). In Melgaço, L & Monaghan, J. (eds.) *Protests in the Information Age,* 21-39. London: Routledge.

Dhlela, D. (2020). Military surveillance endangers democracy. *NewsDay.* Available from: https://www.newsday.co.zw/2020/03/military-surveillance-could-endanger-democracy/.

Fernandez, L.A. & Huey, L. (2009). Is resistance futile? Thoughts on resisting surveillance. *Surveillance & Society*, 6(3): 199-202.

Foreign Policy (24 June 2018). Beijing's Big Brother tech needs African faces: Zimbabwe is signing up for China's surveillance state, but its citizens will pay the price. Available from: https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/

Fuchs, C. (2011). New media, web 2.0 and surveillance. *Sociology Compass*, 5(2): 134-147.

Gramer, R., Detsch, J. & Haverty, D. (21 May 2020). China's building projects in Africa are a spymaster's dream. *Foreign Policy.* Available from: https://foreignpolicy.com/2020/05/21/china-infrastructure-projects-africa-surveillance-spymaster-dream/

Hawkins, T. (1981). Factional fighting flares up in Zimbabwe: Clash of Mugabe, Nkomo groups threatens stability. *Christian Science Monitor.* Available from: www.csmonitor.com

Hove, M. (2019). When a political party turns against its cadres: ZANU-PF factional infightings 2004-2017. *African Security,* 12(2): 200-233.

Human Rights Watch. (2018). Zim NGO Bill restricts operations. Available from: https://www.pambazuka.org/governance/zimbabwe-ngo-bill-unacceptable

Lindsay, J.R., Cheung, T.M. & Reveron, D.S. (2015). *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. New York: Oxford University Press

Makumbe, J. (2009). *The impact of democracy in Zimbabwe: Assessing political, social and economic developments since the dawn of democracy*. Harare: UZ Publication Office.

Maringira, G. (2017). Politicization and resistance in the Zimbabwean National Army. *African Affairs,* 116(462): 18-38.

Masunungure, E. (2020). *Zimbabwe's Trajectory: Stepping Forward or Sliding Back*. Harare: Africa Book Collective.

Media Institute of Southern Africa (MISA). (15 September 2018). *Zimbabwe government steps up surveillance*. Harare: MISA.

Media Policy and Democracy Project Report (MPDP) (2019). Drifting towards darkness: An exploratory research of state surveillance in post-2000 Zimbabwe. Available from: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/zimbabwe_report_2nd_pages.pdf

Moon, T.H., Heo, S.Y., Lee, S.H., Leem, Y.T., & Nam, K.W. (2015). An analysis on the appropriateness and effectiveness of CCTV location for crime prevention. World Academy of. Science, Engineering and Technology. International . Journal of Social and Behavioural 1;9(3): 836-43.

Mozur, P., Jonah, M., Kessel, J.M., & Chan, M. (2019). Made in China, exported to the world: The surveillance state. https://www.oodaloop.com/briefs/2019/04/24/made-in-china-exported-to-the-world-the-surveillance-state-video/

Munoriyarwa, A. & Chiumbu, S.H. (2020). Big Brother is watching: Surveillance regulation and its effects on journalistic practices in Zimbabwe. *African Journalism Studies,* Special Issue, pp. 1-16.

Nehanda Radio (12 May 2019) Russia seeks military cooperation, diamond, platinum projects in Zimbabwe. Available from: https://www.reuters.com/article/us-zimbabwe-russia/russia-seeks-military-cooperation-diamond-platinum-projects-in-zimbabwe-idUSKCN1GK2JK

NewsDay (12 September 2018). Government installs CCTV without consultation. Available from: https://www.techzim.co.zw/2018/08/chinese-firm-to-install-surveillance-cameras-in-harare/

NewsDay (23 March 2020). *Zimbabwe: Army boosts surveillance capabilities as civil unrest looms*. Available from: https://www.worldaware.com/resources/blog/special-report-zimbabwe-widespread-civil-unrest-unlikely-near-term

Ochieng' Opalo, K. (2019). *Legislative development in Africa: Politics and postcolonial legacies*. Cambridge: Cambridge University Press.

Ottaway, M. (2013). *Democracy challenged: The rise of semi-authoritarianism*. Washington: Carnegie Endowment.

Richards, J. (2012). Intelligence dilemma? Contemporary counter-terrorism in a liberal democracy. *Intelligence and National Security,* 27(5): 761-780.

Rohrlich, J. (2020). Chinese nationals caught surveilling same US military base twice in 2 weeks. Available from: https://www.realcleardefense.com/2020/01/09/chinese_nationals_caught_surveilling_us_military_base_twice_in_2_weeks_311563.html.

Ruhanya, P. (2019). Militarisation of state institutions and the November military coup. Available from: www.theindependent.co.zw-of-state-institutions-and-the-november-military-coup

Rupiya, M. (2011). The military factor in Zimbabwe's political and electoral affairs. *SW Radio Africa*. Available from: http://www.swradioafrica.com/Documents/The%20Military%20Facto r%20in%20 Zimbabwe.pdf

Sachikonye, L.M. (2011). *When a state turns on its citizens: 60 years of institutionalised violence in Zimbabwe*. Harare; African Books Collective.

Tendi, B.M. (2019) The EU's Zimbabwe dilemma. *The Guardian*. Available from: https://www.theguardian.com/commentisfree/2009/sep/13/eu-zimbabwe-sanctions-zanu-pf

Tendi, B.M., 2020. The motivations and dynamics of Zimbabwe's 2017 military coup. *African Affairs*, 119(474): 39-67.

The Herald (9 September 2019). Zimbabwe: Chinese tech revolution comes to Zimbabwe Available from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiosePegZjrAhWsSxUIHZTCBMMQFjAAegQIAhAB&url=https%3A%2F%2Fallafrica.com%2Fstories%2F201910090185.html&usg=AOvVaw3LEEazK_7J9f53RhwKzlQK

The Telescope (12 September 2015). Iran gives Mugabe spy-technology. Available from: https://bulawayo24.com/index-id-news-sc-national-byo-61558-article-iran+gives+mugabe+spy-technology.html

The United Nations Human Rights Office (2017). Dangerous practice of digital mass surveillance must be subject to independent checks and balance. Available from: www.ohchr.org

The Zimbabwe Independent (14 June 2019). Civil society leaders on military watch list. https://www.theindependent.co.zw/2019/06/14/civil-society-activists-on-military-watch-list/

The Zimbabwe Independent (2 June 2018). How factional tug-of-war evolved. Available from: https://www.theindependent.co.zw/2017/09/15/factional-tug-war-evolved/

The Zimbabwe Independent (24 March 2018). Panicky ZNA deploys army units. Available from: www.theindependent.co.za-how-tug-war-evolved

Veritas (2019). Lethal force and the use of the military to maintain order. Available from: http://veritaszim.net/node/3378

Waples, S., Gill, M. & Fisher, P. (2019). Does CCTV displace crime?. *Criminology & Criminal Justice*, 9(2): 207-224.

Warren, I. (2015). Surveillance, criminal law and sovereignty. *Surveillance & Society*, 13(2): 300-305.

Zimbabwe Coalition on Debt and Development (ZimCoDD) (2018). *Zimbabwe: ZimCoDD corners Gvt over "unknown" debts*. Available from: http://www.publicdebtnet.org/pdm/.content/News/News-01313.html

Zimbabwe Lawyers for Human Rights (2017). Enforced disappearances: An information guide for human rights defenders and CSOs. Available from: https://www.zlhr.org.zw/wp-content/uploads/2016/10/Enforced-Disappearances-An-Information-Guide-for-Human-Rights-Defenders-and-CSOs.pdf

Media Policy and Democracy Project

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

Visit mediaanddemocracy.com for more information.

This report was supported by a grant from Luminate.