CHAPTER NINE

A civilian-driven model for surveillance oversight in Zimbabwe

Allen Munoriyarwa

Introduction

The bombing of the Twin Towers[1] in the United States on the morning of 11 September 2001 is often infamously remembered as a 'recognisable icon of terrorist wickedness' (Brown, 2011, n.p.). The London bombings of 7 July 2005[2] are also infamously touted as '. . . deadly attacks on civilisations by extremist cowards . . .' (ITN Archive, 2023). In Mozambique, Ali (2021) has argued that the Islamic insurgency in Cabo Delgado province is a result of the intelligence failures of the State Information and Security Services (SISE). In these three cases that I highlight here, there is an overarching motif that ties them together – that intelligence can fail, much to the detriment of a country. The failure of intelligence agencies is a consequence of a multifaceted set of factors, including organisational deficiencies that hinder intelligence agencies from performing their functions. Organisational deficiencies manifest themselves in several ways. These include a lack of preparation, an inability to grasp the ever-changing demands of surveillance and

1 The story can be followed here: https://www.britannica.com/event/September-11-attacks.

2 It can be followed here: https://www.britannica.com/event/London-bombings-of-2005.

security intelligence, a lack of resources and a lack of accountability for intelligence agencies (Ali, 2021). After the 9/11 bombings, Thomas Kean (The National Commission on Terrorist Attacks Upon the United States – Panel Chairman) summed up these failures rather instructively, thus: 'We were unprepared. We did not grasp the magnitude of a threat that had been gathering over a considerable period of time. As we detail in our report, this was a failure of policy, management, capability, and, above all, a failure of imagination' (quoted Ali, 2021).

While the lack of intelligence imagination is mentioned by Thomas Kean above, and lack of preparedness, failure of policy, and management capabilities are all existential threats to intelligence, I want to argue in this chapter that in Zimbabwe, the increasing politicisation of intelligence agencies, and the political polarisation within these agencies that often follows as a consequence of politicisation, are the major causes of intelligence failures. Because of this politicisation, intelligence agencies in the country have acted partisanly, targeting civil society activists and opposition party leaders. In addition to this, because of internal political polarisation these agencies target other members of the same ruling party that they defend. Such activities constitute intelligence overreach and, as Patel (2019) notes, intelligence overreach should be viewed as failure. Thus, in the Zimbabwean context, intelligence agencies have become obdurate, partisan and opaque and, consequently, have lost much legitimacy in public opinion because they are now seen as an appendage weaponised to prop a faltering and beleaguered ruling party. This constitutes a mission creep. Added to this are the Zimbabwe Defence Forces (ZDF) intelligence agencies that have also become involved in illegal civilian surveillance in the service of ZANU-PF (see Moyo, 2018; Ruhanya, 2020; Media Policy and Democracy Project [MPDP] 2019 and 2021). Currently, the CIO and the ZDF are increasingly involved in digital surveillance practices, which go beyond their purview as national security agencies. How did we arrive here? In this chapter, I seek to answer three questions:

1. How did intelligence agencies, especially the CIO, become a political appendage of the ZANU regime?

2. How can these surveillance institutions be held accountable for their actions?
3. What pathways exist to bolster collective civilian inclusion in surveillance regulation?

I draw on Patel's (2019) argument that surveillance overreach is supposed to be understood as a failure of agencies. In addition to this, I also draw on an argument I made earlier (see Munoriyarwa, 2022) that the politicisation and subsequent polarisation of surveillance agencies constitute failure. In so doing, I want to extend an argument that I make (see Munoriyarwa, 2022; and forthcoming – 2025), and many other scholars, (for example, Moorcraft, 2012; Chan, 2019), that the Central Intelligence Organisation (CIO), Zimbabwe's premier intelligence agency, has declined in terms of efficiency. It has become rotten from the inside and has become a political appendage of ZANU-PF, the ruling party, which uses it as an instrument to retain power, by haunting both internal and external opposition to those in power. Elsewhere, other scholars (see Moorcraft, 2012; Moyo, 2014 and Chan, 2019) have noted that the CIO has basically become part of the ruling party, ZANU-PF's apparatus of violence and civilian subordination. For example, Simpson and Hawkins (2018) note that in the 2008 general elections, the CIO saved Mugabe and ZANU-PF from a violent political meltdown by becoming a reactionary apparatus of the party, violently suppressing civilian-led protests against a debilitating economic crisis. Tendi (2016) notes that they were, furthermore, very much involved in the ZANU-PF succession disputes that led to the overthrow of Robert Mugabe in a military coup. All these assertions point to the failure of surveillance agencies. As Gill (2020) and Owen (2012) note, failures like the ones I have outlined here are a result of the failure of oversight. With proper oversight-function mechanisms, the CIO would not have engaged in such blatant and egregious mission creep practices. It means the existing model of oversight has not worked in Zimbabwe. What other oversight models can be practised in order to avoid such failures? Building on these arguments, I extend the debate by examining how, over time, intelligence institutions became weaponised,

politicised and militarised. I further extend the debate by proposing what I call a multifaceted civilian-driven model that can remedy these excesses in semi-authoritarian contexts using Zimbabwe as a point of entry. By semi-authoritarian regimes, I draw on an earlier definition we used (see Munoriyarwa and Chibuwe, 2021). I mean regimes that maintain a facade of democracy but dissolve its substance. For example, they hold periodic elections, which are not free and fair; they set up oversight mechanisms of certain government functions but dissolve some others; they allow many newspapers, but dissolve media diversity. Furthermore, semi-authoritarian regimes politicise, manipulate and weaponise state institutions to maintain political power and hegemony. Semi-authoritarian regimes often weaponise state security agencies to maintain internal tranquillity within their own parties. In other words, state security agencies within these regimes can be used in a partisan manner to prop one faction of the ruling party against another.

This chapter is organised as follows. In the next section, I provide a background to this research. In this background, I want to highlight two critical incidents of intelligence failure in Zimbabwe that form the central pivots and entry points of my argument. They are critical incidents in the sense that they signify the irrelevance/non-existence of the oversight mechanism in Zimbabwe, or rather, expose its absence. Furthermore, they are critical in that they clearly pointed out what ails Zimbabwe's intelligence, and hence make a clear case for the need for reform. After this, I provide a literature review, where I discuss African scholarship on intelligence oversight. The review is followed by the conceptual framework. To understand the issues I discuss in this chapter, it is important to conceptualise oversight. This section is followed by a brief methodology of the chapter. I then provide my findings and conclude with a discussion.

Background

Zimbabwe is increasingly contending with a slew of digital surveillance practices ranging from location surveillance, public-space surveillance and many more (MPDP, 2019; MPDP, 2021). The CIO has been,

historically, responsible for much of this surveillance on civilians (MPDP, 2019). As such, credible reports have noted that the agency has purchased different surveillance technologies from as far as China and Iran. For example, in 2012 there are reports (see *The Zimbabwean*, 2019) that the CIO purchased email-hacking technologies from Iran. There were also reports (see Hawkins, 2018) that the CIO had purchased some IMSI catchers from China. Government security ministries justify this range of practices by arguing that they are necessary as crime-fighting measures and protection of the country from powerful colonial forces. However, the uses of these technologies come against a background of three other developments (Munoriyarwa, 2022). These are (a) an insufficient understanding of their use by both the public and the institutions administering most of these technologies; (b) regulatory gaps that leave room for abuse; and (c) the weaponisation of surveillance practices that lend the practice to political rather than intelligence uses (Ndlela, 2019; 2020). There are no known civilian-inclusive conversations about surveillance governance in the country and, consequently, the practice operates in a black-box manner (Munoriyarwa, 2024). The Interception of Communication Act (2007) provides the CIO with powers to undertake surveillance. There are also constitutional protections for civilians, at least on paper. Regulatory measures that protect surveillance from being practised in intrusive and covert ways are available on paper but not practised. For example, sections 207 to 210 of the Zimbabwe Constitution protect individuals and legitimate political parties from unlawful surveillance. Furthermore, section 207(2) is clear that surveillance agencies are subject to parliamentary oversight. Yet, despite this, there are no mechanisms to hold these institutions to account. There are also no practical regulatory mechanisms that ensure the legality and transparency of surveillance. Sections 224 to 226 of the Constitution of Zimbabwe prohibit the CIO from engaging in party politics. In addition to this, Section 210 prohibits the military from engaging in party politics as well. However, in reality, this has not been the case. There are incidences of surveillance of activists that have been reported in Zimbabwe.[3] Even as far back as early 2000, Mugabe's

3 For example, as reported here: https://www.theafricareport.com/336723/

critics were already targeted for surveillance. For example, the outspoken former Archbishop of the Roman Catholic Church, Pius Ncube, was surveilled using cameras, and all fingers pointed at the CIO. Mugabe even announced the revelations before the state-controlled media. This was part of the evidence that Mugabe knew of this long before the exposés. The same treatment was meted out to long-time fierce opponent of Mugabe, Morgan Tsvangirai of the opposition MDC which had been formed in 1999 and successfully opposed ZANU-PF (see *The Zimbabwean*, 2012). At the height of the succession disputes that finally deposed Mugabe, senior party members of the ruling ZANU-PF were scared that they might have been watched by the CIO (Munoriyarwa, 2021b). Recently, the cases of opposition leader Job Sikhala and Vice President Kembo Mohadi have demonstrated critically how the ruling party continues to abuse intelligence and strengthened the argument for the need for oversight beyond the flimsy provisions of the Constitution.

In August 2020 the Zimbabwe Republic Police (ZRP), the ZDF 'Ferret Unit'[4] started hunting renowned opposition leader Job Sikhala. The military units were very active in this hunt, according to people with knowledge about the unit. Much of the information on Job Sikhala's whereabouts was received from surveilling his cell-phone activities. The unit went as far as his rural home of Dema, a few kilometres from Harare.[5] The MPDP (2021) had earlier noted that the military's capabilities of surveillance in Zimbabwe were growing, bolstered by Chinese start-up technology companies that were supplying the ZDF with these technologies. The second critical incident I want to refer to is the Kembo Mohadi resignation of 2021. In 2021, Kembo Mohadi resigned from the Vice Presidency (VP) of Zimbabwe. In his resignation letter, he pointed out some very crucial

zimbabwe-digital-rights-activists-fear-misuse-of-surveillance-cameras-in-bulawayo/. And here: https://www.newsday.co.zw/theindependent/tennis/article/15765/zim-in-danger-of-sleepwalking-into-a-surveillance-state.

4 A combined force of CIO, ZRP and military agency specialising in surveillance.

5 The story dominated social-media platforms as the Ferret intensified the hunt for Job Sikhala. Public discussions about the hunt for Job Sikhala can be followed here: https://web.facebook.com/share/p/o5BcXG8Q7WL5bjh5/.

details that could not be lost to any surveillance researcher. The VP instructively said, in a letter that is now in the public domain, 'I am a victim of information distortion, voice cloning, and sponsored spooking and political sabotage . . .' [6] It is instructive to note that the VP reveals political sabotage manifesting itself in sponsored spying. These two incidences are the most recent ones that point to a persistent history of state intelligence abuse. However, they are not the only ones. In this chapter I draw on these two because of their currency, but in order to provide a clear picture of abuse of state intelligence. I also draw on historical incidences of state intelligence abuse littered across the state intelligence's history in Zimbabwe. Where do we point the fingers of scorn? One commentator[7] noted that there are deeper issues in this resignation that the leadership cabal should confront. One of these deeper issues would be, if the VP is subjected to voice cloning and sponsored spooking, how safe are we as ordinary citizens? One important point to note in these two incidences is that there was no public outcry about the snooping to which Kembo Mohadi was subjected, or about how Job Sikhala was also treated. Much of the outrage remained in elite debates. The public was generally left out of these debates. There are two questions worthy of reflection after these incidences: would these incidences have taken another dimension if the public had been conscientised about these and what is it they could have done? This leads to the question: how can we best bring the public into these debates?

Beyond the questions I have raised and reflected on above, these two important incidences highlight several issues. First, they show the growth of intelligence surveillance and its misuse to suppress dissent, as seen in the case of Job Sikhala, how it may be used to influence leadership changes within the ruling party. Second, these events are critical in that they revealed the limited influence of civil society on

6 Mohadi's full resignation letter is available here: https://www.herald.co.zw/breaking-vice-president-mohadi-resigns/ and here: https://www.voazimbabwe.com/a/kembo-mohadi-resigns/5797207.html.

7 The commentator remarked here: https://www.voazimbabwe.com/a/kembo-mohadi-resigns/5797207.html.

rolling surveillance back and holding the government to account. Third, they point to the fact that in Zimbabwe, intelligence agencies are weaponised through a process of 'Zanufication' – where they serve the ruling party ZANU-PF. Furthermore, these incidences are critical in that, within ZANU-PF itself, they removed all doubt that might have existed under Mugabe, as to whether the CIO serves specific factions of the ruling party. This is in addition to these agencies spooking on legitimate civil society and opposition.

Furthermore, these incidences point to the fact that in such regimes, like Zimbabwe, where the ruling party benefits politically from surveillance practices by state institutions, regulatory bodies should be reconfigured in order to ensure adherence to global standards of surveillance that seek to maintain surveillance as an intelligence practice, and not a political one. There is limited evidence of effective public responses to these incidents and, where they have occurred, they have been confined to a few civil society organisations, like Zimbabwe Human Rights NGOs, and have not been deeply rooted in Zimbabwean society. I, therefore, propose a civilian-driven surveillance oversight model that can be applied in (semi-)authoritarian regimes. But before proposing such a model, I want to examine the genesis of this mission creep. How did we get to this point, where intelligence agencies are politicised, factionalised and weaponised against legitimate civil society actors and political-party activists?

This chapter draws on two sets of data. Primarily, it draws on 16 in-depth interviews with several actors with an interest in state intelligence and surveillance regulation and oversight. These interviewees were drawn from members of the last National Assembly (NA) (some of whom remained in the 2023 parliament) from both the ruling party and the opposition (formerly known as the Citizens Coalition for Change, formerly led by Nelson Chamisa). There were precisely seven members of Zimbabwe's NA interviewed. Three were formerly of the ruling party, ZANU-PF, and four from the opposition. Three interviewees were lawyers, two were members of network service providers and two were civil society activists who work in the field of digital rights and privacy. Lastly, two were journalists. For anonymity, which was guaranteed, they will be coded as part of this analysis. Among

other issues, the interviewers sought to ask the respondents: how did the politicisation of Zimbabwe's intelligence agencies happen? The interviewers also sought to understand the extent to which these agencies still serve national security; the effectiveness of the oversight mechanisms available; and what can be done to ensure oversight and accountability of intelligence agencies. These are some of the questions they were asked. These interviews will be augmented by document analysis, drawing on credible news reports, CSO reports and any other credible documents available. For data analysis, document analysis will be used, drawing on credible information drawn from the documents analysed. The interviews will be subjected to thematic analysis that draws out major themes from the interview data.

Oversight of Zimbabwe's security agencies

Zimbabwe's CIO, a civilian agency, is constituted in Section 207 of the country's 2013 Constitution. This section states that Zimbabwe has four primary security agencies: the Zimbabwe Defence Forces (ZDF), the police services (Zimbabwe Republic Police [ZRP]), the CIO and the Prisons and Correctional Services. However, in Section 207 (e), an Act of Parliament can provide for establishing other security services. It is important to note that the CIOs are part of the country's security establishment. Furthermore, it is important to note that the ZRP and ZDF have separate intelligence agencies. For example, the ZRP's internal intelligence agency is called the Police Internal Security and Intelligence (PISI). PISI is supposed to focus on internal police intelligence, while the ZDF's intelligence unit should focus on military-related intelligence. The prisons and correctional service have their own internal intelligence unit. The senior commanders of ZRP, ZDF, CIO and prisons all constitute the Zimbabwe National Security Council (NSC) in terms of Section 209 of the Constitution. The NSC, chaired by the president and including the two Vice Presidents, ministers and members of the security services, is responsible for strategic security planning and coordination. The Constitution of Zimbabwe provides for both executive and parliamentary oversight of the intelligence agencies. As stated earlier,

section 209 provides for the NSC, which the president chairs. Section 210 is named 'Independent complaints mechanism' and it states, 'An Act of Parliament must provide an effective and independent mechanism for receiving and investigating complaints from members of the public about misconduct on the part of members of the security services and for remedying any harm caused by such misconduct.'

The intelligence-gathering and surveillance activities of the CIO are policed by the 2007 Information Communication Act (ICA) law. There are three very important clauses in Section 6(1), which are articulated in Hungwe and Munoriyarwa (2024) as follows:

> A warrant (for surveillance) shall be issued by the Minister to an authorised person . . . if there are reasonable grounds for the Minister to believe that
>
> (a) Any of the following offences has been or is being or will probably be committed (i) a serious offence by an organised criminal group.
>
> (b) . . . the gathering of information concerning an actual threat to national security or to any compelling national economic interest is necessary.
>
> (c) The gathering of information concerning a potential threat to public safety or national security is necessary.
>
> In exercising the above, the minister and the CIO are governed by Section 208 of the Constitution, which provides for the conduct of the security services. Section 208 states that no security agent shall:
>
> (a) act in a partisan manner
>
> (b) further the interests of any political party
>
> (c) violate fundamental rights and freedoms
>
> (d) prejudice the lawful interests of any political party.

These constitutional clauses are further fortified by Section 208 (c), which is clear that no members of the security services shall be active office bearers of any political party and that no member of the security service shall be employed by the civilian institution(s). There are several points to note in these clauses. Section 210 provides for

an independent complaint mechanism. Admittedly, this is oversight, but it does not go far enough to encompass issues like the CIO budget, their intelligence-gathering activities of the year, their capabilities and an assessment of the credibility of the threats they investigate. The section focuses on complaints specifically. In practice, this oversight does not even exist, even in attenuated form. This has allowed the CIO and other intelligence agencies to operate with impunity. Recent incidences demonstrate this impunity, which thrives as a consequence of this lack of oversight. On 29 December 2023, the PISI summoned the veteran journalist and Director of the Information for Development Trust (IDT), Tawanda Majoni, to Harare Central Police. The IDT is an investigative-journalism hub that supports the local and Southern African media and journalists in probing corruption, human-rights abuses and socio-economic violations relating mostly to the public sector. It was formed in 2015 and, since then, has helped scores of journalists produce more than a hundred investigative stories exposing malpractices in the public and private sectors.[8] The second incident involves the president, Emmerson Mnangagwa. On 10 November 2023, Mnangagwa announced that he had appointed the Commander of the ZDF, General Phillip Valerio Sibanda, to the ruling party's highest decision-making body, the politburo. This blatantly violated Section 208 (a and b) of the Constitution, as read with 208 (clauses 3 and 4). It was human-rights lawyer Kudzayi Kadzere who threatened to sue the president if he did not annul the appointment. There was no quest for explanation from any parliamentary oversight body after these two incidences. For example, General Sibanda was appointed on 10 November, and the appointment was subsequently annulled on 23 November. No parliamentarian in the two weeks that followed requested any explanation despite the egregious violation. This demonstrates lapdog oversight, or rather, its absence in a captured parliament. In addition to this, Section 6(1) gives powers to the Minister of State Security; there is a provision for parliamentary oversight and to determine warrants. On the other hand, the NSC, in terms of Section

8 This story can be followed here: https://zimbabwe.shafaqna.com/EN/AL/1717875 and here: https://www.newsday.co.zw/thestandard/news/article/200021454/undercover-police-summon-investigative-journalism-hub-director.

209, is chaired by the president. What this means is that while, on paper, there is a provision of parliamentary oversight, it does not exist in practice, but executive oversight is given preponderance through Section 6(1) and Section 209 of the Zimbabwean Constitution. This has opened up intelligence agencies to executive influence.

Intelligence accountability and oversight in Africa

Literature on surveillance oversight is still emerging. Hutton (2009) notes that notions of accountability (and by extension, oversight) are a relatively new phenomenon in African states. Hutton (2009, p. 1) further argues that this is because:

> The intelligence sector has traditionally been viewed as a core arena of state security outside of the purview of parliament and civil society. As democratic arrangements have become more entrenched and oversight of the security sector has improved, space has opened for debate on the functions and practices of intelligence.

The works of Duncan (2018; 2022) constitute part of this emerging foundational literature. Broadly, Duncan (2018; 2022) makes the overarching argument that, without oversight, surveillance can be abused for political purposes. The abuse of the South African intelligence by former president Jacob Zuma is telling evidence of this possibility even in countries deemed to be democracies (Duncan, 2018). Without oversight, Duncan (2022) argues, there are several risks that can easily debilitate intelligence agencies, for example, as noted previously, their politicisation. However, there are further risks that include internal decline, corruption, power struggles and outright failure of intelligence (Duncan, 2022). Elsewhere in Africa, the Africa Defence Forum (ADF, 2023) has argued that the increasing growth of surveillance technologies across most African countries requires vigilance in oversight of end users – the intelligence agencies. The ADF argues that this immense growth of surveillance technologies empowers intelligence agencies, but requires corresponding powers of oversight (ADF,

unpublished). Kuwali (2023) agrees with ADF, noting that intelligence and security agencies need oversight to ensure that they are subject to the law. Kuwali (2023) agrees with Duncan (2018; 2022) that weak oversight of intelligence agencies can inhibit professionalism. The parliament of South Africa (n.d.) has noted that oversight is critical for other aspects like control of surveillance practices, which stops rogue surveillance agencies from conducting unwarranted surveillance, accountability and budgetary control. The agreement in this literature is that there is a need for oversight and accountability to avoid intelligence overreach and excesses like the targeting of legitimate political opponents, activists, communities and journalists. There is also a need, as the available literature suggests, to institute oversight of the intelligence institutions to guard against internal turmoil, politicisation, corruption and rogue intelligence agencies. Much of the literature on surveillance oversight in Africa is still in policy briefs, rather than academic empirical research (see, for example, Hutton, 2009; Kuwali, 2023) and newspaper briefs (see, for example, ADF, 2023). Duncan's (2018; 2022) remains the most recent intellectual work on intelligence oversight on the continent. This points to the existence of a huge gap in the need for more empirical research on the subject. Southern African researchers, particularly in Zimbabwe, Mozambique, Zambia and Malawi, have not mustered much research on intelligence oversight. This chapter attempts to fill this gap by examining possible routes of intelligence oversight in a Zimbabwean context.

Understanding oversight as a practice

The debate on oversight often takes different dimensions, depending on the context. In Africa, for example, where the demand for oversight of the intelligence agencies is still emerging, policymakers and activists are still grappling with the question of why, in the first place, oversight of the intelligence agencies is needed (Hutton, 2009) and, related to this question is its historical origin (Wegge, 2017). In advanced democracies these questions are fairly settled. The debates are now around what kind of oversight and what it can do to intelligence agencies. Intelligence oversight is

part of a process that ensures some form of both transparency and accountability for intelligence services (Glees, 2011; Patel, 2019). Generally, there are two types of mistakes intelligence agencies can make (Brown, 2011) that require oversight. The first one is the failure to detect threats in advance (Brown, 2011; Goldman and Rascoff, 2016). The Pearl Harbor attack,[9] the 9/11 and the London bombings of 7 July 2005 are examples of how intelligence agencies can fail, and how oversight can hold them to account, and flag internal weaknesses that can lead to these failures. Such a failure is a consequence of several factors, including, chiefly, the collection of wrong information, erroneous assessments of intelligence information, inaccurate information and a lack of adequate resources (Brown, 2011). The second level of failure that requires oversight is abuse of power (Goldman and Rascoff, 2016; Mare and Munoriyarwa, 2026). Oversight ensures that intelligence agencies do not infringe on civil liberties and human rights in the name of national security (Brown, 2011). Oversight is useful to flag down aggressive protection of citizens that does not adhere to laws, including indiscriminate collection of data for mass surveillance. Intelligence oversight, therefore, is not only about setting the rules for intelligence agencies. It is about whether the rules have been complied with and whether they are providing an outcome that was intended of them (Brown, 2011; Kamarck, 2021). In the era of technology, oversight is meant to ensure that surveillance agencies are using technologies properly and not using these technologies to thwart legitimate political activities or to gather intelligence that may lead to the torture and harassment of citizens. Beyond these two issues, oversight is also necessary to check the unnecessary expansion of intelligence agencies, which might lead to an ever-growing burden on the fiscus (Brown, 2011). More so, oversight is a form of check on the politicisation and capture of intelligence agencies by ruling regimes.

Intelligence oversight is, therefore, about whether intelligence agencies are undertaking their mandated duties and operating

9 The Pearl Harbor attack can be followed here: https://www.britannica.com/study/timeline-of-the-attack-on-pearl-harbor.

within the constraints of both domestic and international law (Breakspear, 2012). It is an oversight mechanism put in place to thwart rogue behaviours by intelligence agencies. Enduring questions of oversight include whether the oversight required should be executive oversight or an independent mechanism of checks and balances. But the question of whether intelligence oversight should be by the executive or by an independent system is very important in semi-authoritarian contexts like Zimbabwe, where the executive has politicised intelligence agencies and subordinated them to their shaky regimes as part of regime-defence mechanisms. In these regimes, the question becomes, how then can civilians be protected from all too powerful regimes and intelligence agencies? In these regimes, surveillance overreach, which should be policed by a robust oversight mechanism, is often justified in public discourse as part and parcel of the protection against external threats (Munoriyarwa, 2022). When voices are raised against overreach, an ill-founded justification is asserted – 'too much' oversight of the intelligence agencies can harm national interests. According to Breakspear (2012), research has shown that in most contexts, civilians do not often have keen interests in intelligence and its practices. This, arguably, is often a result of the fact of their deliberate and strategic exclusion by the elite. Because of this strategic exclusion of civilians from intelligence oversight, intelligence agencies easily slip from being state institutions to political-party appendages. To understand oversight in semi-authoritarian regimes like Zimbabwe, we first need to understand the genesis of this gradual process of Zanufication of intelligence. Then, we can examine possible pathways to oversight of the intelligence agencies. It can be argued that parliamentary oversight is in itself a form of civilian oversight. But the problem with semi-authoritarian regimes is that the parliaments are captured and exists in attenuated form to be of use in oversight.

Findings

The first section of the findings will address the mutation of Zimbabwe's intelligence agencies into political appendages of the ruling ZANU-PF party. The second section will suggest alternative pathways of oversight that can work to rein in these intelligence agencies that are increasingly being politicised and weaponised against political options, journalists and activists. For the first question, I trace the overt politicisation and weaponisation of the intelligence agencies to a historical factor, namely Robert Mugabe's authoritarian designs of post-independence Zimbabwe, and the structure of the intelligence agencies he inherited, that synced neatly with the colonial edifice of intelligence agencies that he inherited. Secondly, the worsening factionalism within ZANU-PF, which precipitated actors within the party to collapse into state intelligence agencies. This increasing factionalism of ZANU-PF was punctuated by an external development – growing opposition to ZANU-PF leadership. This also precipitated the ruling party to collapse and depend on state intelligence agencies, and weaponise them to fight legitimate civil society and political opposition.

The Historical Genesis of the 'Zanufication' of State Intelligence Agencies

Firstly, how did the state intelligence agencies, especially the CIO, mutate into violent party-aligned intelligence agencies? To understand the contemporary capture of Zimbabwe's intelligence agencies, one needs to understand the history of intelligence agencies themselves, in colonial Zimbabwe. (The country was referred to as Rhodesia before independence.) A close look at the country's intelligence agencies would show that the postcolonial intelligence agencies, military intelligence and the CIO are two sides of the same coin. The main purpose of intelligence agencies is the preservation of national security. National security is a valence issue – an ideal shared by all political players. However, in colonial periods in Zimbabwe the CIO's role went beyond this. While the intentions of

setting it up were to preserve national security by pre-empting attacks through intelligence gathering, the CIO became a political appendage of the Rhodesian Front (RF), the ruling party of the colonial era. Ken Flower established the CIO under the colonial Prime Minister Winston Field (Megahey, 1998), although the discussion to set up an agency had started long before under the Prime Minister Edgar Whitehead. Even though Ken Flower always saw himself as apolitical (Preston, 2004), his activities became very much political. For example, his alleged direct involvement in setting up a militant movement (RENAMO) to counter FRELIMO in Mozambique (Alao 2012). Thus, from its formation, the CIO meddled in politics and became part of the institutional mechanisms on which the RF drew its political powers to manage increasingly restive and militant colonised Black populations in the country (Matthews, 1999). The idea was to weaken and destabilise Mozambique's role as a host of Zimbabwe's guerrilla movement but, in addition to this, to save the RF as a ruling party as well. Thus, while the colonial CIO's role can still be located within the realm of security intelligence, its politicisation was rooted in its formation in 1963. It was also, furthermore, manned by RF sympathisers of varying commitments.

This is the CIO Robert Mugabe inherited from Ian Smith, the last minority-government Prime Minister, first as Prime Minister and secondly as President, until his deposition in a coup in 2017. For a start, Mugabe briefly retained Ken Flower as the director of the intelligence agency. This retention was easy to justify in the public domain, as it could be seen as ensuring continuity of a leader with institutional memory for easy transition in an agency that needed careful reform. But, beyond this, the retention was an early harbinger of Mugabe's intentions of the CIO. One respondent notes:

> If you want to understand the behaviour of the CIO today, you should trace it back to the 1980s when Mugabe inherited it from Smith. Mugabe's intentions were clear. He did not want to reform the CIO. He already saw an opportunity to keep it as it was – a political organisation that could serve his political ends (Informant 12 MNA, interview in Harare).

Mugabe's intentions to maintain the status quo were, however, not misplaced. We need to understand, first, Mugabe, the individual, as a political player. One of Mugabe's erstwhile allies in the 1980s, Edgar Tekere, described Mugabe as a brutal, manipulative and vindictive political architect who had no intention to step down once he took over power in 1980, as Prime Minister. His quest was for absolute power (Tekere, 2007). With no institutional restraints in this quest for power, Mugabe was inexorably drawn to security institutions to manipulate. What made Mugabe's quest for total power worse was the fact that the Constitution had not fortified security institutions from the reach of an overzealous executive or a ruling political party. For example, measures of independence that exist in other countries, such as public interviews for security institutions' heads by a parliamentary committee, did not and still do not exist. Thus, Mugabe's quest for power was inadvertently aided by a Constitution that did not offer any measure of restraints nor fence off certain institutions from the overreaching political hand of the executive. One lawyer notes:

> Mugabe was never restrained from the start. The CIO was not the only institution that he manipulated. Mugabe aimed at all institutions that would potentially restrain his quest for total power. In the CIO and the military intelligence, Mugabe installed people whom he could control and who were also his allies. People like Mkandi and Chipanga [former CIO directors] were firm Mugabe allies . . . this was for me the beginning of the descent to politicisation of the CIO . . . and you know it also happened with military intelligence . . . (Informant 1, Lawyer, Interview in Johannesburg).

The process of politicising the intelligence agencies was not only driven by Mugabe's relentless pursuit of total power, but by his enablers in both the government and security services. Chief amongst these enablers included ministers and military commanders. For example, researchers Burke (2018) and Matyszak (2018) note that Emmerson Mnangagwa, the current president, was the 'go-to fix it' person (n.p.) for Mugabe. These are the people, within the ruling party, who pushed Mugabe's project to capture and 'Zanufy' state

institutions like intelligence services. A report[10] on intelligence notes that with the help of his numerous enablers, Mugabe weeded out perceived internal opponents in the CIO. These include elements of the Zimbabwe People's Revolutionary Army (ZIPRA), a guerrilla movement led by nationalist Joshua Nkomo, that had also fought, alongside ZANU-PF, for the liberation of Zimbabwe. The report notes thus:

> [Mugabe] . . . "weeded out from CIO in a very systematic way because they [former ZIPRA officials: ZIPRA was ZAPU's military wing during the liberation struggle] were passing intelligence to Dumiso Dabengwa (ex-ZIPRA intelligence chief) and Swazini Ndlovu, who was Dabengwa's number two". By 1987, when the Zanu PF and ZAPU hostilities were resolved through the signing of the Unity Accord that subordinated the latter to the former, CIO was dominated by ex-ZANLA (ZANU's military wing during the armed struggle that liberated Zimbabwe) personnel – an outcome that underscored a new form of politicisation in CIO. The number of ex-Rhodesian operatives had also dwindled by 1987, with the retirement of the divisive Flower being the most significant single departure.

When the expulsion of internal opponents was completed, and allies had been installed in influential positions within these security agencies, Mugabe's total control and the Zanufication of these agencies was complete.

Factionalism in the ruling party and state intelligence capture

One important factor that drove ZANU-PF leaders to politicise intelligence agencies was factionalism. In 1980, when Mugabe assumed the prime ministership, he was not the only popular poli-

10 This report is accessible here: https://www.zimbabwesituation.com/news/zimsit-m-cio-a-history-of-politicisation-division-and-internal-suspicion-the-zimbabwe-independent/.

tician. There was Joshua Nkomo, who, I argue, was even more popular than Mugabe. Nkomo's ZAPU had won 24 seats out of the 80 common roll seats contested. Mugabe's ZANU-PF had won 57 out of the 80, but this victory had always been attributed to the party's use of violence. The existence of ZAPU flew in the face of their total quest for hegemonic dominance in Zimbabwe. A military solution was devised, and it led to the Gukurahundi massacres of the early 1980s, a military operation launched in the early 1980s in Matabeleland and parts of Midlands where ZAPU support was dominant (Burke, 2018).

There are four important consequences that can be drawn from the Gukurahundi massacres of the early 1980s. At a societal level, it was an unwarranted loss of innocent lives and one of the earliest expressions of violence by the Mugabe regime. At a political level, Mugabe was able to subdue his opponents, both real and imaginary. For example, the ZAPU leader Joshua Nkomo was left with no option but to sign a unity accord with ZANU to form ZANU-PF. The involvement of the military in the massacres and the intelligence agencies drew these institutions close to Mugabe. This flirtation of security and military agencies with ZANU's political power endured hitherto. Lastly, and perhaps more importantly, Gukurahundi demonstrated, vicariously, to all political players, how Mugabe intended to deal with his opponents in the future, regardless of whether the opposition was legitimate or otherwise. As one informant noted:

> The covert and overt involvement of the military and the CIO in the Gukurahundi massacres was a turning point for intelligence services in the country. The first lesson to me was that these agencies were willing to fight from Mugabe's corner. The second one was that after the Gukurahundi crimes, they were now beholden to Mugabe. Mugabe had their dossiers, and no one could afford to stray . . . (Informant 6: MNA, Zoom interview).

The politicisation of the intelligence services was, therefore, complete with the capture of the senior leaders of the organisation. In the post-Gukurahundi period, the politicisation and weaponisation of the intelligence agencies has continued unabated. For example,

senior and junior officers of the CIO have been accused in numerous reports of the torture of activists acting to protect ZANU-PF, the then President Mugabe, and this protection has continued even in the so-called second republic. Even internal opposition within ZANU-PF, has been targeted for surveillance. The targeting of former army General Solomon Mujuru, who was now in the ZANU-PF Party sums up how partisan the intelligence service had become. Tendi (2016, n.p.) sums up what Mugabe then said about Mujuru:

> . . . Mugabe said to me: 'Bonyongwe [former head of the CIO] is (General) Mujuru's man. I want to know what (General) Mujuru is doing (in Zanu PF), so create a parallel intelligence structure for spying on (General) Mujuru and bring that information directly to me. Every time I met Mugabe alone, he always asked what (General) Mujuru was doing. He was very worried that (General) Mujuru would remove him from power.

As Zimbabwe's elections became more competitive after 2000, the CIO had become more aggressive in protecting a hugely unpopular ruling ZANU-PF party. They have also been the violent force of the ruling party, cited in numerous credible reports about election violence in Zimbabwe. Some security officers have testified[11] openly, after leaving the force, about how the state intelligence abducts civilians in furtherance of ZANU-PF's political dominance by force. The CIO had become a blatant force on ZANU-PF's behest. Their history of interfering with elections and supporting ZANU-PF is now well documented. For example, a report[12] published before the 2023 elections showed that the incumbent president, afraid of factionalism within his ruling party, had leaned heavily on the CIO to stifle the opposition, because trust in his allies was declining, due to

11 One such testimony can be followed here: https://www.zimeye.net/2020/10/18/former-state-security-officer-tells-how-zimbabwe-state-intelligence-executes-abductions/.

12 This report can be followed here: https://www.zimeye.net/2020/10/18/former-state-security-officer-tells-how-zimbabwe-state-intelligence-executes-abductions/.

factionalism in the party. The 2023 elections were later widely condemned by observers, including the Southern African Development Community's (SADC) own observer mission.[13] One former member of the national Assembly noted:

> It is now common knowledge that Mugabe and Mnangagwa now militarised the CIO and have weaponised it into their weapon against the opposition. We have long known that the CIO has no credibility as an intelligence agency . . . where in Zimbabwe have you mentioned the name CIO and you hear respect and adoration? Nowhere except in ZANU-PF circles. They are ruling party militias, actually (Informant 16, MNA, interview in Harare).

Scholars have long noted (see the numerous works of Tendi, 2016; 2019) on intelligence agencies in Zimbabwe, that the complete capture of the intelligence agencies worked together with their militarisation. For example, Tendi (2016, n.p.) states:

> Bonyongwe has held the director-general post since 2003, meaning that military officers have led CIO for approximately two decades now. Yet CIO is a civilian institution manned by career intelligence officers. The imposition of military officers without a civilian intelligence background irked ambitious long-serving civilian intelligence operatives . . .

The recent spying on Job Sikhala, which I have described above, is a continuation of how ZANU-PF treats legitimate opposition using state intelligence. The spying on Kembo Mohadi, which he himself testified to, is also a testimony of internal factionalism within the party itself. However, the growing opposition to ZANU-PF rule, by both organised political parties and CSOs, has driven the capture of state intelligence to extreme levels. Since 1980, ZANU-PF had lost support because of its handling of the

13 The issue is documented here: https://africacenter.org/spotlight/sadc-navigate-zimbabwe-election/.

economy, corruption, human-rights abuses and many other misdeeds (Ruhanya, 2018). In the next section, we discuss how opposition to ZANU-PF has accelerated the intelligence-capture project.

External opposition to ZANU-PF as a driver of intelligence politicisation

ZANU-PF had never enjoyed unified support for its rule. In the previous section, I explained internal opposition to its rule. But external opposition had also often posed a threat to ZANU-PF's hegemony. Digital surveillance against external opponents to the ZANU-PF regime takes three major dimensions. The first one is illegal digital surveillance by the CIO targeted at individuals within state-controlled institutions who are important to the survival of ZANU-PF in power, but whose loyalty is doubted. An example is the now widespread surveillance of editors of state-controlled media houses. I consider this to be surveillance of external opposition because they are not (ruling) party members, even though they are an important cog in the party's grand design to retain power. As far as 2008, the CIO was already spying on editors of state-controlled media houses (Reporters Without Borders [RWB], 2009). This was mainly conducted through hacking their emails, especially the private emails. This points to the fact that the CIO from as far back as early 2000 possessed the capability to hack emails. The MPDP (2019) pointed out this practice. RWB (2008) confirmed this practice in the case of editor Bhekinkosi Ncube of the state-controlled magazine *Umthunywa*. RWB (2008, n.p.) reports this widely:

> He is alleged to have insulted President Mugabe in an email sent from his private email address. The accusation is baseless and proves only that his personal email was monitored. We call for his reinstatement, the destruction of all the gathered data and an investigation into the government's violation of the Interception of Communications Act . . . During a hearing on

> the case on 7 October in Harare, Zimpapers CEO Justin Mutasa revealed that he had placed all of his editors under electronic surveillance to establish whether they supported ZANU-PF. He authorised the use of password-cracking software to hack into their private email accounts. The Interception of Communication Act allows the government to tap phone calls and monitor email and fax communications in order to 'guarantee national security' but does not authorise hacking into private email correspondence without a warrant.[14]

One journalist interviewed states that the electronic hacking of private emails was rampant in state media houses, but, 'We all know this is not done by the media institutions' leadership themselves . . . we know it is the work of the CIOs who are spying on us' (Informant 7, Journalist; telephony interview).

CIO surveillance of these journalists and editors is based on ZANU-PF's desire to ensure these journalists remain loyal to the party and are not sharing any information they might come across with other people (MPDP, 2019; Munoriyarwa, 2021; Munoriyarwa, 2021; Munoriyarwa and Chiumbu, 2022). For state-controlled media, the surveillance has worsened because:

> [They] . . . have been suspected of leaking dirty information about the CIO to the international media and international organisations . . . The CIO is convinced that it is only the state-controlled editors and senior journalists who are privy to their operations and some of their illegal activities . . . you know, last year the CIO were aware of exposures being prepared by an organisation called The Sentry[15] . . . they went for broke because they wanted to identify suspected collaborators . . . (Informant 7, Journalist, telephony interview).

14 The RWB story can be followed here: https://rsf.org/en/government-spied-email-state-owned-newspaper-editors-august.

15 The Sentry finally published the report in June 2024. It is available here: https://thesentry.org/reports/cio-business-network-zimbabwe/.

The second dimension of this surveillance is against senior political opposition leaders. Growing opposition to ZANU-PF by organised political parties has also pushed ZANU-PF to consolidate its grip on the CIO and its politicisation of the institutions for ZANU-PF's narrow partisan interests. In post-2000 Zimbabwe, as the economy imploded, ZANU-PF found itself cornered. Its own structures were no longer viable in the communities from which it drew its support. This precipitated CIO surveillance on opposition leaders. It is now known that Mugabe's long-time opponent, Morgan Tsvangirai, was subjected to surveillance through email hacking, and his alleged love story was exposed.[16] There is no doubt that this was the work of the state intelligence agencies, as there are no private players who could be allowed to possess this technology. In an interview in 2019, one former security agency official had said, 'This capability is owned by the military and the CIO. It has been used in several cases, and it is often targeted at the opposition.'[17]

Another former opposition leader, Eddie Cross, a member of the former MDC National Executive, once complained publicly about how the CIO had hacked his emails. He was quoted by *The Zimbabwean* newspaper as saying this:

> Firstly, I cannot accept that the *Herald* [state-controlled newspaper] obtained my e-mail and the response from Kerry Kay from a 'leak' within the party. My e-mail was sent to five members of our leadership – the President, the Secretary General, the Treasurer and the National Spokesperson, as well as Mrs Kay, a member of our National Executive. Not one of these individuals would have, under any circumstances, leaked an e-mail of this nature to the state-controlled media. I must therefore assume that these were routine intercepts by State

16 The story of Morgan Tsvangirai email hacking can be followed here: https://www.newsday.co.zw/thestandard/politics/article/228676/pm-marriage-saga-takes-new-twist.

17 The respondent is quoted form a previous MPDP report available here: https://www.dailymaverick.co.za/article/2017-11-15-zimbabwe-army-in-control-of-state-institutions-but-insists-not-a-coup/.

> Security Agents. I note this with interest and will make sure to use other means for communications of this nature in future (Source: *The Zimbabwean*, 24 March 2014)

The third and final dimension in the digital-surveillance matrix is surveillance targeted at CSOs. I use the term 'civil society' to include church leaders who have been surveilled as a consequence of their criticism of the ZANU-PF regime. CSOs have long been subjected to surveillance from Mugabe's regime to the current so-called second republic. One CSO activist noted:

> If you are in the field of human rights defence and political activism, then you do not need to be informed that you are under both physical and digital surveillance. It is certain that the CIO will follow you . . . even if you go to the airport, they follow . . . You need to be cautious in the digital space as well . . . (Informant 15, Zoom interview).

Church leaders critical of ZANU-PF have also been targeted for surveillance. The former Roman Catholic Church leader in Zimbabwe, Archbishop Pius Ncube, is a case in point. Pius Ncube was a fierce Mugabe critic. In July 2007, 'Ernest Tekere, a former Central Intelligence Organisation operative who planted cameras in the bedroom of Archbishop Pius Ncube and captured the Catholic priest romping with his personal assistant.'[18]

In 2007, *AllAfrica* reported the same story, noting that there was a conspiracy between the state-controlled media and the CIO to torment Mugabe's critics. The paper reported:

> Details of a plot hatched by the CIO spy agency working hand in hand with state media journalists have emerged, with indications that the two worked hand in glove in planning and exposing the adultery story involving Archbishop Pius Ncube. Archbishop Ncube was slapped with a $20 billion adultery

18 The full story is reported here: https://twitter.com/zimlive/status/1401952609850773504.

> lawsuit at St Mary's Cathedral a month ago after he was served with the papers by the Deputy Sheriff, who was accompanied by a large contingent of journalists and photographers from the state media (AllAfrica, 25 August 2008).

The chronicle I have provided here provides irrefutable evidence of intelligence abuse by the ruling party, ZANU-PF. What I have demonstrated is that the CIO, from its formation in 1963, has always been a political appendage of the party in power. It has been beholden to the leadership in power. Tendi (2016) had demonstrated that in the twilight of Mugabe's rule, the CIO had been a central actor in the succession matrix. This all paints a clear picture of state intelligence abuse by the ruling party, and a mission creep on the part of the intelligence agencies. Tendi (2016) notes that since independence in 1980, the CIOs have been led by former military people with unquestionable loyalty to Mugabe. Building on Tendi's argument, I had argued (Munoriyarwa, 2022) that the imposition of military personnel on civilian agency adds another dimension of militarisation to an already politically compromised intelligence agency.

The CIO, evidently, had abandoned its duty of state security and protection of citizens to become an aggressive and violent abuser of these rights in the service of the ruling party. What do these abuses and the mission creep by the CIO point to? There is one clear answer to this question: these points indicate a lack of oversight of the CIO, which, in turn, perpetuates a lack of accountability. As one opposition MNA notes:

> The CIO is a rogue institution. It cannot be held accountable by anyone . . . even the members of the ruling party we talk to acknowledge in private that the institution is abused . . . it reports to the president only . . . what kind of an institution can that be? You remember, even during the GNU, we wanted this institution either dissolved and shed of its ZANU-PF operatives or brought to account by constitutional amendments. Mugabe and his ZANU-PF flatly refused (Informant 10, interview in Harare).

What worsens this situation is that ZANU-PF, already afraid of revelations of past abuses, will not agree to any form of accountability on the CIO. On 18 August 2011, a privately-owned radio station, SW Radio, released a list of names[19] from the CIO, who were said to be either involved in corruption linked to ZANU-PF or tortured opposition and civil society members. The list included names allegedly known in the CIO for past alleged transgressions in defence of the ruling party. For example, Joseph Mwale was indicted by the High Court in Zimbabwe for the alleged murder of two opposition leaders, Talent Mabika and Tichaona Chiminya.[20] Other CIO operatives on the list produced by SW Radio for alleged political and economic crimes included Keeper Nyambanje, David Nyika, Sidney Somai and Jeffrey Tabva. This complicates any moves towards oversight. There are just:

> Too many skeletons in the CIO cupboard. There is no one there who wants to operate transparently . . . most of them [the CIO as an agent, not those listed above as SW Radio published mere allegations] are either corrupt, work with individuals in ZANU PF . . . or have committed crimes of their own. I do not think there is an oversight that they would want . . . (Informant 8, interview in Harare, MNA).

Even under these circumstances that are likely to stir resistance from within the CIO and the ruling party, there is still an imperative need, given the abuses examined in the preceding sections, to attempt oversight.

Pathways to oversight of intelligence

There are two issues that I have established here: a well-established culture of intelligence abuse by the ruling party, and the absence of

19 The list of these names is in the public domain. It can be accessed here: https://nehandaradio.com/2011/08/18/more-cio-agents-exposed-in-extra-list-2/.

20 The High Court indiction is also available in this story: https://allafrica.com/stories/200605190272.html.

parliamentary oversight of intelligence agencies. So, what oversight pathways exist for a semi-authoritarian regime like Zimbabwe, with evidently no oversight of its intelligence agencies, and well-documented abuses of intelligence powers? There are, obviously, no clear approaches. The first question would be: who should conduct oversight? The absence of parliamentary oversight and ZANU PF's dominance of parliament means that even if constitutional guardrails of oversight are eventually established, they are likely to reproduce the same ineffectual oversight they are meant to avoid.. With a few opposition members in the national assembly, the parliamentary oversight model will not work. Through the second amendment, ZANU-PF now controls the judiciary. The capture of the Zimbabwean judiciary by the ruling party ZANU-PF has been documented widely.[21] This means it is foolhardy to rely on judicial pronouncements for directions for intelligence agencies' oversight. The courts have become ZANU-PF appendages, like the CIO itself (Tembo and Singh, 2023). The second question is: for the CIO, what should oversight achieve? The answer to this question is fairly straightforward. Firstly, oversight would rein in the CIO from targeting non-state-security actors like politicians, CSO activists, journalists, and so on. Oversight will, furthermore, help ensure that the CIO fulfils its expected mandate of safeguarding national security. This would represent effective deployment of national resources for money for the Zimbabwean taxpayers. In addition to this, oversight ensures that the CIO follows the laws, its own policies, regulations and ethical guidelines and turns it away from being a rogue and criminal political outfit, which, currently, is feared and distrusted by citizens.

I would like to propose a multivariate or hybrid oversight model for surveillance oversight that can be useful in the Zimbabwean context. I call it multivariate/hybrid in the sense that it proposes to bring together various actors from different segments of society into one oversight institution established by an act of parliament. Furthermore, the model takes into consideration three current political realities of the Zimbabwean context. Firstly, it realises that in its

21 For example, in this report: https://www.theafricareport.com/51602/zimbabwe-mnangagwas-capture-of-judiciary-a-red-flag-for-state-failure/.

current form, parliament is weak and partisan (in favour of ZANU-PF) to constitute a standing oversight mechanism on its own. Secondly, it recognises that, given the high levels of corruption and other nefarious activities, the CIO itself would most likely resist any oversight structure that excludes its representation. Thirdly, the oversight structure I propose under the multivariate/hybrid model recognises the incorrigibility of the Executive to any reform that targets the security cluster in general, and the CIO, because they constitute the source of their political power. The ruling ZANU-PF executive would most likely construe any oversight proposal as a 'biblical Samsonian[22] trick' to weaken them. To give it power, this oversight institution would be enabled by an act of parliament. Its effectiveness lies in the fact that it encapsulates actors from different practices, including CSOs. These actors are likely to jolt into action hitherto lethargic actors like MNAs. Also, MNAs who might fear acting on intelligence for fear of political backlash can exercise autonomy and action in a committee that involves several other players.

However, a multivariate model would include five actors important to intelligence oversight. In the Zimbabwean case, it would include representatives from the CIO itself, especially the top Director, the Executive, for example, a permanent secretary or some senior personnel, parliamentary representatives, in which opposition parties in parliament should be represented, and representatives of CSOs, including lawyers, human-rights defenders, surveillance experts and privacy experts. The debate would be: how much power should this institution have? My proposal is it should be given statutory powers to approve budgets, examine warrants that have been issued over a period of time they determine, deliberate on appointments and promotions, oversee the roll-out of surveillance technologies by both state and private actors, be privy to surveillance technologies' purchase decisions made, among other issues. I further propose that the CSO representatives in this structure be given extra statutory responsibilities to form a subcommittee that deals with investigating citizens' complaints against the CIO. In terms of parliamentary representation, I propose that each political party that polls about 20 per cent of the

22 In the Bible Samson's enemies targeted his hair to weaken him physically.

national vote be represented in this oversight committee. The Constitution of Zimbabwe, in Section 210, allows parliament to establish other intelligence agencies. This clause can be useful in allowing this new creature I am proposing here, investigative powers in the case of abuse. In other words, this model proposes capacitating the oversight structure to appoint and commission investigations into intelligence agencies, with a mandatory clause being added that if such an investigation is commissioned, it should be tabled before a stipulated time expires and made available (except for confidential material) to the public. This proposal is a compromise between the potentially secure judicial oversight, which I argue and have argued elsewhere (see Munoriyarwa, 2022) the Executive will never accept, and the non-existent executive oversight with its failings. The diagram below illustrates how the oversight structure I propose would work.

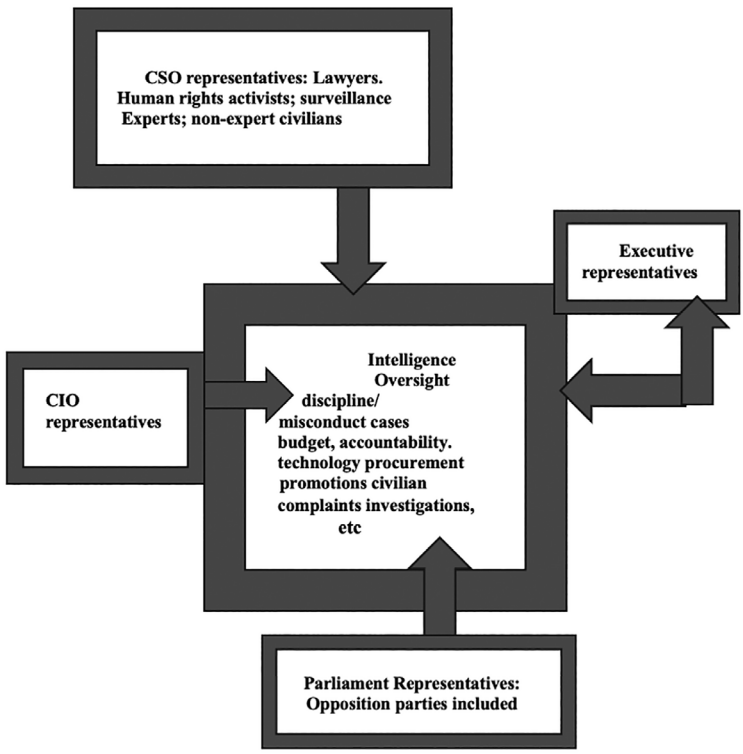

Figure 9.1: An illustration of a multivariate/hybrid model for intelligence oversight in a semi-authoritarian context like Zimbabwe. © Author.

This, by far, is not a perfect model. And it is a new structure. But in a political context where the state is dominated by the ruling party, weaponising intelligence agencies, bringing in civilians in the oversight can help to hold them accountable, and bring about transparency. There are several advantages in bringing civilians into an oversight structure, as I propose in this model. The CIO, as noted earlier, is feared and not trusted by civilians. A model like the one I propose here, if adopted, can change these current perceptions of the CIO. More so, civilians' models of oversight can potentially generate public support for intelligence agencies, which is currently lacking in Zimbabwe. Also, civilian support is necessary for quality intelligence. The CIO, more than any other agency, needs this support.

Discussion and conclusion

The purpose of this chapter was to answer three research questions. These are: how did intelligence agencies, especially the CIO, become a political appendage of the ZANU-PF regime? The second question is, how can these surveillance institutions be held accountable for their actions? Lastly, what regulatory pathways exist to ensure public efficient oversight of intelligence agencies? The chapter drew on critical incidents of surveillance that ended up in the public domain to make a case for a civilian-driven oversight model. The chapter was anchored on two recent incidents that became a national 'spectacle' in the sense that they drew attention to the CIO for the wrong reasons. These were the surveillance of opposition leader Job Sikhala, leading to his arrest and politically motivated detention. The second one was the surveillance of Vice President Kembo Mohadi, leading to his resignation from the position, and his public complaints that he was a 'victim of sponsored spooking'. But to make a solid case of a culture of mission creep and the politicisation and weaponisation of the intelligence agencies, the chapter drew on several historical cases.

Intelligence oversight is by its nature very complex. It becomes even more complicated when civilians are brought on board. For example, an oversight structure that includes civilians may end up

focusing on issues that are not entirely about intelligence or may end up squabbling. But defining and policing the focus of oversight is important from the start. Also, it is important to create specific legislation to consolidate civilian inclusion in oversight of agencies. For example, the terms of reference may need to be properly defined in civilian oversight structures. But attempts to include civilians cannot be abandoned because of these perceived concerns. These concerns may be clarified over time. Clarity, of course, can actually be capital in surveillance-oversight structures. For example, in the context of Zimbabwe, a civilian model, like the proposal I have outlined above, can focus on bringing about transparency and accountability in surveillance through improving performance and conduct. These are not outlandish goals. They are achievable. But there are strong factors that can militate against a civilian-driven oversight of intelligence.

The first factor is that the CIO and ZANU-PF have been mutual partners in the slide to authoritarianism that postcolonial Zimbabwe has witnessed. In fact, the CIO has been an enabler of ZANU-PF's undemocratic hold on power. How can these political 'Siamese twins' be separated? This is the most difficult question. And resistance to any form of oversight is likely. Then, secondly, parliament in its current form, especially after the 2023 elections, is dominated by ZANU-PF. There is little likelihood that ZANU-PF parliamentarians will support a decision that the CIO and the ruling elites do not like. One National Assembly member said:

> Even in the ruling party, people are afraid of the CIO. But you cannot wake up and call for accountability without being recalled and expelled. When we hear opposition members complaining about these people, we understand, but we work under a whip system . . . we cannot do that . . . it has very serious consequences . . . (Informant 14, interview in Harare).

This sums up what can militate against civilian inclusion. There will be obvious resistance from the CIOs themselves and the Executive. But if parliament is not willing to act, then the whole idea of civilian oversight will be difficult to implement. Added to these factors are

three other important issues about the Zimbabwean political context. The first issue is ZANU-PF's exaggerated sense of self-entitlement to the Zimbabwean polity will likely work against anything that brings civilians on board. Added to this is the polarised nature of Zimbabwe's politics that makes it difficult for parties to find common ground and engage in logrolling practices during lawmaking debates. Lastly, trust and suspicion in the polity are still rife. Future research should, perhaps, focus on how civilian trust and awareness about intelligence agencies can be built in order to involve them in intelligence oversight structures.

References

Alao, A. (2012). *Mugabe and the Politics of Security in Zimbabwe*. McGill-Queen's Press-MQUP.

Africa Defence Forum. 2023. Zimbabwe Turns to Chinese Technology to Expand Surveillance of Citizens. *Africa Defence Forum*. [Online]. [Accessed on 2 July 2024]. Accessible at: https://adf-magazine.com/2023/01/zimbabwe-turns-to-chinese-technology-to-expand-surveillance-of-citizens/.

AllAfrica. 2008. CIO, State Media Connive in Ncube Smear Campaign. *AllAfrica*. [Online]. [Accessed 10 May 2021]. Available from: https://allafrica.com/stories/200708250045.html.

Breakspear, S. (2012). *The policy impact of PISA*. Paris: OECD Publishing.

Burke, J. (2018). 'Mnangagwa talks of unity as opposition hides from army.. Accessible at: https://share.google/amocvqdy2dhNSfa2a. Accessed on 12 July 2018.

Chan, S. 2019. *Mugabe: A life of power and violence*. London: Bloomsbury Publishing.

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

Duncan, J. 2022. *National Security Surveillance in Southern Africa: An Anti-capitalist Perspective*. London: Zed Books.

Gill, P. (2020). Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and national security, 35(7),* 970-989.

Glees, A. (2011). European Security Intelligence. In Jorgensen, K. E., Laatikainen, K., Drieskens, E., & Kalland Aarstad, A. The SAGE handbook

of European foreign policy Volume Two, (pp. 264-276). London: SAGE Publications Ltd.

Hawkins, A. 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. *Foreign Policy*. [Online]. [Accessed 13 August 2020]. Available from: https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

Hungwe, B. and Munoriyarwa, A. 2024. An analysis of the legislative protection for journalists and lawyers under Zimbabwe's Interception of Communications Act. *Statute Law Review*. 45(1), hmae018.

Hutton, L. 2009. *Intelligence and accountability in Africa*. [Online]. [Accessed 12 May 2024]. Available from: https://issafrica.org/research.

ITN Archive. 2023. *7/7 London Bombings. Tony Blair and George Bush React to News of Attacks (2005)*. [Online]. Available from: https://youtu.be/xHJL2bL1UgQ.

Kuwali, D. 2023. *Oversight and Accountability to Improve Security Sector Governance in Africa*. [Online]. The Africa Center for Strategic Studies. [Accessed 2 April 2024]. Available from: https://africacenter.org/publication/asb42en-oversight-accountability-security-sector-governance/.

Mare, A. and Munoriyarwa. A. 2026. *Disinformation Campaigns in Africa: Actors, Consequences, and Responses*. London: Bloomsbury Academic Publishers.

Matthews, R. O. 1999. *Civil Wars in Africa: Roots and resolution*. Montreal: McGill-Queen's University Press.

Matyszak, D. (2018). Mugabe: Mnangagwa's permanent friend. *ISS Today*. (30, n.p. no issue) Accessible at: https://share.google/Lm3XBrJhVlapdN4k4. Accessed on 8 April 2024.

Media Policy and Democracy Project (MPDP). 2019. *Drifting towards darkness: An exploratory research of state surveillance in post-2000 Zimbabwe*. [Online]. [Accessed 20 July 2020]. Available from: https://www.dailymaverick.co.za/article/2017-11-15-zimbabwe-army-in-control-of-state-institutions-but-insists-not-a-coup/.

Megahey, A. 1998. *Humphrey Gibbs, Beleaguered Governor: Southern Rhodesia, 1929-69*. London: Palgrave Macmillan.

Moorcraft, P. 2012. *Mugabe's War Machine*. Johannesburg: Jonathan Ball Publishers.

Moyo, G. 2014. Understanding the executive-military relations in Zimbabwe: beyond Mugabe's redistributive nationalist rhetoric. *Journal of African Union Studies*. 3(2_3), pp. 69–86.

Munoriyarwa, A. and Chiumbu, S.H., (2020). "Big Brother is Watching: Surveillance Regulation and its Effects on Journalistic Practices in Zimbabwe". *African Journalism Studies*, 40(3), pp. 26–41. DOI: https://doi.org/10.1080/23743670.2020.1729831.

Munoriyarwa, A. 2021a. The growth of military-driven surveillance in post-2000 Zimbabwe. *The Media Policy and Democracy Project May 2021*.

Munoriyarwa, A. 2021b. When watchdogs fight back: resisting state surveillance in everyday investigative reporting practices among Zimbabwean journalists. *Journal of Eastern African Studies*. 15(3), pp. 421–41.

Munoriyarwa, A., (2021a). 'When Watchdogs Fight Back: Resisting State Surveillance in Everyday Investigative Reporting Practices Among Zimbabwean Journalists' *Journal of Eastern African Studies* 15 (3), pp. 421-441. DOI: https://doi.org/10.1080/17531055.2021.1949119.

Munoriyarwa, A. 2022. The militarization of digital surveillance in post-coup Zimbabwe: 'Just don't tell them what we do'. *Security Dialogue*. 53(5), pp. 456–74.

Munoriyarwa, A. and Chibuwe, A. 2022. Journalism beyond the coup: Emerging forms of digital journalism practices in post-coup Zimbabwe. *Digital Journalism*. 10(7), 1, pp. 198–218.

Munoriyarwa, A. and Chiumbu, S.H. 2019. Big brother is watching: Surveillance regulation and its effects on journalistic practices in Zimbabwe. *African Journalism Studies*. 40(3), pp. 26–41.

Munoriyarwa, A. and Mare, A. 2023. *Digital Surveillance in Southern Africa*. Cham: Palgrave Macmillan.

Ndlela, D. 2020a. 'Zim's era of the state' could herald increased repression. *The Standard*. [Online] [Accessed 20 June 2022]. Available from: https://www.thestandard.co.zw/2020/09/06/zims-era-of-the-state-could-herald-increased-repression/.

Ndlela, D. (2020). Zim in danger of sleepwalking into a surveillance state. Available from: https://www.newsday.co.zw/theindependent/tennis/article/15765/zim-in-danger-of-sleepwalking-into-a-surveillance-state. Accessed on 20 June 2021.

Owen, M. D. (2012). A review of intelligence oversight failure: NSA programs that affected Americans. *Military Intelligence Professional Bulletin 4,* pp.33-34.

Patel, F. 2019. Homeland Security's Intelligence overreach: Two cases illustrate risks to civil society. [Online]. *Just Security*. [Accessed 3 June 2024]. Available from: https://www.justsecurity.org/63116/dhs-surveillance-reveals-oversight/.

Preston, M. 2004. *Ending Civil War: Rhodesia and Lebanon in Perspective*. London: Taurus Academic Studies.

Reporters Without Borders. 2009. *Internet Enemies – Countries under surveillance: Zimbabwe*. [Online]. [Accessed 13 July 2024]. Available from: https://www.refworld.org/reference/countryrep/rsf/2009/en/64570.

Ruhanya, P. 2018. Militarisation of state institutions and the November military coup. *Zimbabwe Independent*. [Online]. 17 November. [Accessed 14 June 2022]. Available from: www.theindependent.co.zw-of-state-institutions-and-the-november-military-coup.

Ruhanya, P. 2020. The militarisation of state institutions in Zimbabwe, 2002–17. In: Ndlovu-Gatsheni, S.J. and Ruhanya, P. eds. *The History and Political Transition of Zimbabwe: From Mugabe to Mnangagwa*. London: Palgrave Macmillan, pp. 181–204.

Simpson, M. and Hawkins, T. 2018. *The Primacy of Regime Survival: State Fragility and Economic Destruction in Zimbabwe*. London: Palgrave Macmillan.

Tekere, E. 2007. *A lifetime of struggle*. Harare: SAPES Books.

Tembo, S. and Singh, A. 2023. Mutilation of the independence of the judiciary: threats, intimidation and constitutional amendments in Zimbabwe. *Obiter*. [Online]. *44*(3), pp. 546–60. [Accessed July 13, 2024]. Available from: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1682-58532023000300003&lng=en&tlng=en.

Tendi, B.M. 2016. State intelligence and the politics of Zimbabwe's presidential succession. *African Affairs*. 115(459), pp. 203–24.

The Standard. 2020. Creating a surveillance state: ED govt zooms in for critics with Chinese. 1 March. *The Standard*. [Online]. [Accessed 14 September 2021]. Available from: https://www.thestandard.co.zw/2020/03/01/creating-surveillance-state-ed-govt-zooms-critics-chinesehelp/.

The Zimbabwean. 2014. Emails must have been hacked. *The Zimbabwean*. [Online]. [Accessed on 12 April 2020]. Available from: https://www.thezimbabwean.co/2014/03/e-mails-must-have-been/.

Wegge, N. and Wentzling, T. 2017. Contemporary and Future Challenges in Effective Intelligence Oversight. In: Leigh, I., & Wegge, N. Eds. *Intelligence oversight in the twenty-first century: accountability in a changing world* (1st ed.). Oxford: Routledge. https://doi.org/10.4324/9781351188791.