



iStock
Credit: NatanaelGinting

October 2025

ZIMBABWE'S SURVEILLANCE STATE

Facilitating an omnipresent tyranny



CONTENT

<i>Executive Summary</i>	3
<i>Introduction</i>	4
 <i>Surveillance Laws in Zimbabwe: From Colonial Control to Digital Authoritarianism (1890-2025)</i>	 X
<i>Foreign Enablers of Surveillance</i>	24
<i>Surveillance and its impact on elections and democracy in Zimbabwe</i>	29
<i>Journalism under attack</i>	36
 <i>Conclusion</i>	 40



EXECUTIVE SUMMARY

This report provides a comprehensive analysis of Zimbabwe's transformation into a surveillance state under successive Zimbabwe African National Union Patriotic Front (ZANU-PF) administrations, with particular emphasis on the technology-aided acceleration of these practices, under current President Emmerson Mnangagwa's regime (2017-present).

The report demonstrates how practices initially designed for counterinsurgency and political control by the-then white minority governments in Southern Rhodesia have been continually repurposed and expanded, yielding a sophisticated system of authoritarian governance that fundamentally undermines democratic institutions and human rights well into the 21st century.

Zimbabwe's democratic space has contracted significantly since independence from Britain and white minority rule in 1980. This contraction continues and has accelerated through the expansion of the state's surveillance architecture targeting politicians from both the ruling party and the opposition, civil society actors, journalists and ordinary citizens. Surveillance has evolved from being a reactive, adhoc tool of crisis management to a pre-emptive and central pillar of state governance.

The state employs a multi-faceted and multi-pronged surveillance strategy encompassing physical monitoring, digital surveillance, intelligence infiltration of political parties and civic organisations and systematic data collection through telecommunications infrastructure. The surveillance apparatus

operates through three primary institutions: the Central Intelligence Organisation (CIO),¹ the military intelligence (MI) arm of the Zimbabwe Defence Forces (ZDF),² and the Zimbabwe Republic Police (ZRP).³ These security agencies function with minimal, if any, oversight and broad legal authority granted through legislation such as the Interception of Communications Act (2007) and the Cyber and Data Protection Act (2021).

Founding independence leader Robert Mugabe's regime relied on a mix of colonial-era secrecy laws (e.g. the Official Secrets Act) and institutions such as the CIO and laid the foundations for digital surveillance. While current President Mnangagwa has retained many of the colonial and Mugabe-era repressive laws and institutions, his administration is distinguished by a *qualitative escalation*, that is, the incorporation of digital surveillance technologies, mass data interception, and biometric electoral monitoring. Where Mugabe built the scaffolding of authoritarian control, Mnangagwa engineered a technologically enhanced surveillance apparatus that monitors, anticipates, and neutralises threats in real-time.

1 The African Crime & Conflict Journal, *Intelligence Files: Zimbabwe's Central Intelligence Organisation*, 2023, <https://theafricancriminologyjournal.wordpress.com/2023/01/15/intelligence-files-zimbabwes-central-intelligence-organization/>

2 Sabelo J. Ndlovu-Gatsheni, *Nationalist-Military Alliance and the fate of democracy in Zimbabwe*, Accord AJCR 2006/1, <https://www.accord.org.za/ajcr-issues/%EF%BF%BCnationalist-military-alliance-and-the-fate-of-democracy-in-zimbabwe/>

3 Zimbabwe Human Rights Forum, *Communications and Political Intelligence Surveillance on Human Rights Defenders in Zimbabwe*, 2014, https://www.hrforumzim.org/wp-content/uploads/2024/11/BPUK15104_Insides.pdf

Surveillance often precedes and enables repression: it has facilitated arbitrary arrests, abductions, torture, enforced disappearances, and extrajudicial killings, illustrating the systemic entanglement of intelligence gathering with coercive state violence.⁴ Consequently, pervasive surveillance has cultivated and engendered widespread fear among citizens and produced chilling effects across civic life including reduced participation in democratic and civic spaces,

self-censorship by journalists and a decrease in investigative journalism.⁵

Several survivors of state sponsored surveillance and the resultant brutality report enduring trauma, paranoia, and mistrust, underscoring the longterm psychosocial effects of authoritarian surveillance.⁶ Many others are either fearful or too traumatised to share their experiences at the hands of Zimbabwe's security agents.

4 Chiedza Mlingwa, Tariro Senderai & Fortune Kuhudzehwe, The News Error! A preliminary report on Post-election Organised Violence and Torture: 23 August to 30 September 2023, Human Rights NGO Forum, <https://www.hrforumzim.org/wp-content/uploads/2023/10/The-new-error-Collation-of-Post-Election-OVT-23-August-to-30-September-2023.pdf>

5 Murray, Fussey, Hove, Wakabi, Kimumwe, Saki, Stephens, The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe, *Journal of Human Rights Practice*, Volume 16, Issue 1, February 2024, Pages 397-412

6 Interviews with abduction and torture survivors, Harare, 2025

INTRODUCTION

Zimbabwe presents an interesting case study of “competitive authoritarianism”⁷—a hybrid regime that maintains the institutional trappings of democracy while systematically undermining its substantive foundations.

On the face of it, the country exhibits the formal characteristics of a functioning democracy: regular quinquennial elections have been conducted without fail since independence, international election observers are routinely permitted access, and the textbook tripartite institutional framework—executive, legislature, and judiciary—ostensibly provides the constitutional checks and balances fundamental to democratic governance. The adoption of a new constitution in 2013, approved through a national referendum and marketed as a “people-driven” democratic reform, further reinforced this superficial democratic legitimacy.

However, a closer examination reveals a more troubling reality beneath this democratic veneer. Zimbabwe demonstrates how post-colonial African states can strategically deploy surveillance technologies and manipulate legal frameworks to consolidate authoritarian control while preserving the institutional façade of democratic governance. Under President Mnangagwa’s administration, which assumed power following Robert Mugabe’s military-assisted removal in November 2017, the country has experienced an unprecedented expansion of state surveillance capabilities. This phenomenon represents both institutional continuity with the repressive apparatus inherited from the Mugabe era and a qualitative escalation

of authoritarian practices enabled by technological advancement.

This transformation aligns with wider global patterns of what scholars have conceptualised as “digital authoritarianism”—the systematic deployment of information and communication technologies to strengthen authoritarian governance structures while suppressing political opposition and civil society dissent.⁸ Zimbabwe’s case assumes particular analytical significance because it demonstrates how resource-constrained states can nonetheless develop sophisticated surveillance capabilities through strategic partnerships with external technology providers—particularly China⁹ and Israel¹⁰—and the adaptive manipulation of existing legal and regulatory frameworks.

The Mnangagwa administration has systematically modernised Zimbabwe’s surveillance infrastructure through four principal mechanisms: namely, the integration of Chinese surveillance technologies and expertise through bilateral cooperation agreements; the expansion and refinement of legal frameworks governing communications interception and data collection; the progressive militarisation of intelligence-gathering operations across civilian institutions; and the strategic weaponisation of ostensibly regulatory bodies, most notably the Postal and

7 Levitsky, Steven, and Lucan A. Way. 2010. *Competitive Authoritarianism: Hybrid Regimes after the Cold War*. Cambridge: Cambridge University Press.

8 Feldstein, 2019; Polyakova & Meserole, 2019

9 Advox, How Zimbabwe is building a Big Brother surveillance state, Global Voices Advox, January 10, 2023, <https://advox.globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/>

10 Suraya Dadoo, The seven African governments using Israeli cyberespionage tools, African Arguments.org, February 23, 2021, <https://africanarguments.org/2021/02/the-seven-african-governments-using-israeli-cyberespionage-tools/>

Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), transforming them from neutral oversight entities into instruments of state surveillance and control.

This report provides a comprehensive analysis of Zimbabwe's transformation into a surveillance state under successive Zimbabwe African National Union Patriotic Front (ZANU-PF) administrations, with particular emphasis on the technology-aided acceleration of these practices, under current

President Emmerson Mnangagwa's regime (2017-present). The report demonstrates how practices initially designed for counterinsurgency and political control by the-then white minority governments in Southern Rhodesia have been continually repurposed and expanded, yielding a sophisticated system of authoritarian governance that fundamentally undermines democratic institutions and human rights well into the 21st century.

SURVEILLANCE LAWS IN ZIMBABWE: FROM COLONIAL CONTROL TO DIGITAL AUTHORITARIANISM (1890-2025)

This section traces the evolution of surveillance legislation in Zimbabwe from the colonial era through to the present day, demonstrating how legal frameworks for state surveillance have maintained remarkable continuity across different political dispensations.

Zimbabwe's surveillance apparatus represents one of the most enduring legacies of its colonial past, with legal frameworks established under British colonial rule continuing to underpin state security operations well into the 21st century. This report traces the development of surveillance laws from the establishment of the British South Africa Company (BSAC)¹¹ administration in the 1890s through to contemporary digital surveillance legislation under the incumbent President Mnangagwa. The analysis demonstrates how successive governments have maintained and expanded surveillance powers while adapting legal instruments to meet contemporary challenges to state authority, utilizing both formal intelligence services and informal community-based surveillance networks.

Surveillance has increased to Orwellian levels despite constitutional guarantees for privacy, protection from unwarranted intrusions into personal communications and other individual rights. In terms of the constitution, no one, including the state, has the authority to invade a person's private space or access their communications without due process.¹² However, the state routinely contradicts these constitutional provisions, leading to regular violations of privacy and other individual rights under the guise of law enforcement.

It is the sort of impunity other governments would do their best to hide but not the Zimbabwean authorities. Back in 2014, then Minister of State for National Security Didymus Mutasa publicly boasted that the government, 'sees everything ... we have our

¹¹ John S Galbraith, *Crown and Charter: The early years of the British South African Company*, 1974, https://archive.org/details/british-south-africa-company/CAB%2034-34/?utm_source=chatgpt.com

¹² Veritas, *Constitution of Zimbabwe*, https://www.veritaszim.net/sites/veritas_d/files/Constitution%20Consolidated%20%282023%29.pdf

means of seeing things these days; we just see things through our system. So no-one can hide from us in this country.¹³

Mutasa proceeded to warn Zimbabweans to, 'be careful not to denigrate our president; we will visit your bedrooms and expose what you will be doing.' In 2015 after he had left government, Mutasa said, "Your phones are listened to a lot. The CIO is huge and it produces many reports".

Mutasa's was not an idle boast, Zimbabwe's increasingly sophisticated, pervasive and intrusive surveillance capabilities are built on the foundations laid by colonial regimes and dev eloped by post-independence administrations as outlined below:

EARLY COLONIAL SURVEILLANCE FRAMEWORK (1890-1923)

From its establishment as a settler colony in 1890, the Rhodesian state institutionalised surveillance as both a mechanism of white racial domination and counterinsurgency strategy. Intelligence gathering was not something incidental: it was a core component of a colonial administration aimed at entrenching minority rule and ensuring settler security while simultaneously preventing and delegitimising African political mobilisation.

The colonial surveillance system in Southern Rhodesia was established through a series of legislative acts and the foundational surveillance architecture was built on three key pillars: intelligence gathering, movement control, and information suppression, implemented through both formal institutions and informal networks.¹⁴ At the onset, the newly established colony of Southern Rhodesia was governed through a charter granted to the imperialist Cecil John Rhodes' BSAC by then British Queen Victoria in 1889.¹⁵ The Charter granted the BSAC "all powers necessary for the preservation of public order" (Clause 3) and explicitly authorized the establishment of a police force (Clause 10).¹⁶ These broad provisions gave the chartered government blanket powers to establish an early form of institutionalised surveillance. The British South Africa Police (BSAP) were empowered to monitor, intercept, and censor communication (primarily postal) suspected of instability or sedition. Early statutes also enabled the BSAC to issue "proclamations" with direct force of law—circumventing judicial oversight.¹⁷

In 1894 the Native Regulations Ordinance was passed which established the first systematic surveillance of African populations through the pass system.¹⁸ In 1899 the Masters and Servants Ordinance¹⁹ created mechanisms for monitoring African labour movements. The law criminalised breaches of employment

13 NGO Forum, The Right to Privacy in Zimbabwe, Harvard Law School, 2016, https://humanrightsclinic.law.harvard.edu/wp-content/uploads/2022/10/zimbabwe_upr2016.pdf.

14 Britishonlinearchives.com, Zimbabwe under colonial rule, in Government reports (1897-1980), [https://britishonlinearchives.com/collections/65/volumes/428/administration-1897-1977?filters\[query\]=&filters\[className\]=document](https://britishonlinearchives.com/collections/65/volumes/428/administration-1897-1977?filters[query]=&filters[className]=document)

15 <https://www.rhodesia.me.uk/charter/> accessed on 17/08/2025

16 Rhodesia.me, BSAC Charter, <https://www.rhodesia.me.uk/charter/>

17 Rhodesia.me, Southern Rhodesia Order in Council, October 20, 1898, https://www.rhodesia.me.uk/wp-content/uploads/2018/10/Southern-Rhodesia-Order-In-Council-1898.pdf?utm_source=chatgpt.com

18 Lindsay F Seymour, Legislation affecting Africans in urban areas in Southern Rhodesia, https://journals.co.za/doi/pdf/10.10520/AJA0035483X_115. The pass system required that all black Africans carry identification at all time as a way to control movement and labour; These passes dictated where people could live, work, and travel, and failing to produce them could result in severe penalties, including imprisonment or fines. The system was a form of segregation and a tool for enforcing racial and economic control by the white minority government.

19 Zimbabwe Congress of Trade Unions, About ZCTU, <https://www.zctu.co.zw/about-zctu>

contracts and made it a criminal offense for African workers to leave their jobs without permission. This was a key mechanism for a cheap, captive and monitored labour force. According to the Zimbabwe Congress of Trade Unions (ZCTU), “pass laws were enacted to limit the movement of workers as well as to help enforcing employment contracts,” highlighting the connection between these laws and the control of African labour.²⁰

The Seditious Meetings Act of 1908 prohibited gatherings deemed threatening to colonial authority. This law was modelled on the United Kingdom’s Seditious Meetings Act of 1817 which made it illegal to hold a meeting of more than 50 people for political deliberation without prior notice and authorisation. It gave state officials the power to attend and disperse meetings, with non-compliance leading to felony charges. In British colonies, the law was passed to prohibit public gatherings likely to promote sedition or disturb public tranquillity. It allowed the government to prohibit political meetings and required organizers to give prior notice to the police.²¹ The Seditious Meetings Act thus reflected the colonial government’s belief that effective surveillance required pre-emptive measures against potential political opponents. From the beginning, the state institutionalized what the Italian anarchist writer Luigi Fabbri would term “preventive counter-revolution”—the systematic disruption of potential resistance before it could organize effectively.²² It is clear that the post-independence Mugabe and Mnangagwa regimes copied this preventive template and it continues to inform their approach to dealing with political dissent.

RESPONSIBLE GOVERNMENT ERA (1923–1965)

Responsible Government in Southern Rhodesia introduced self-rule for settlers. The new administration inherited and adapted colonial tools, introducing statutes with more structured surveillance powers.

The Official Secrets Act, first passed in 1923 and subsequently amended in the 1950s, 1960s, and 1970, represents a critical evolution in surveillance legislation from ad hoc company controls to systematic state information management. The act criminalises the unauthorized disclosure of official information and has enabled successive governments to intercept and seize correspondence considered prejudicial to “public safety or order.” The law was adopted by the Zimbabwean government after independence and it remains in use as one of the pillars of the surveillance state.²³ Key Provisions include Section 3 that Prohibits the communication of official information to unauthorized persons; Section 4 covering the “Prohibition of communication of certain information” – which criminalizes unauthorized disclosure; Section 5 that establishes penalties including imprisonment for up to 20 years for violations; and Section 6 that creates presumption of guilt, placing burden on accused to prove innocence.

The Emergency Powers Act²⁴ of 1939 (used extensively during WWII and after) permitted blanket censorship of communication channels and the arrest of individuals without warrant when deemed a “security threat.” It was also used to crack down on politicians

20 Zimbabwe Congress of Trade Unions, About ZCTU, <https://www.zctu.co.zw/about-zctu>

21 UK Parliament, Seditious Meetings Bill volume 35, debated on Monday 10 march 1817, <https://hansard.parliament.uk/Commons/1817-03-10/debates/b7c49791-1755-42c7-994b-977edf567e35/SeditiousMeetingsBill>

22 [The Preventive Counter-Revolution | The Anarchist Library](#) accessed on 19 August 2025

23 Human Rights Archive Zimbabwe, Official Secrets Act (as amended at 31 December 2004) <https://ntjwg.uwazi.io/entity/ghlo6zyho1w?page=5&file=1551255217649kz4k17wzzfn.pdf>

24 UK Parliament, Southern Rhodesia Volume 270: debated on Monday 15 November 1965, <https://hansard.parliament.uk/lords/1965-11-15/debates/2f749e8c-3a51-49c6-809c-05dc09b2dbe2/SouthernRhodesia>

and African trade unionists. Authorities were empowered “without reference to courts” to ban meetings, suppress publications, and confine individuals to specific areas. Significantly, surveillance under this act extended beyond Africans to include left-leaning European settlers and anti-colonial activists, illustrating how laws could be deployed across racial lines whenever the colonial state felt threatened by political actors. This act also testifies to the state’s propensity to adapt its surveillance frameworks to deal with evolving political challenges.

UNILATERAL DECLARATION OF INDEPENDENCE (UDI) ERA UNDER IAN SMITH (1965–1979) ²⁵

On 11 November 1965, then Rhodesian Prime Minister Ian Smith announced the Unilateral Declaration of Independence (UDI) severing ties with colonial power Britain. From then on until 1979, Rhodesia was governed as an ‘independent’ white settler-ruled state. What followed was an intensification of the guerilla war led by African nationalist politicians, including future leader, Robert Mugabe and others, whose aim was the establishment of an independent black majority-ruled state. Faced with an escalation of African political resistance and a guerilla war, the Smith regime responded by escalating and intensifying the Rhodesian state’s surveillance capabilities. Up until the attainment of majority African rule in 1980, the Smith regime was able to entrench a national security state aimed at suppressing political dissent through draconian legal frameworks underpinned by and facilitating surveillance.

Some of the key laws of this era included the Law and Order (Maintenance) Act—LOMA which was enacted in 1960. The Smith administration inherited this draconian law and made full use of it to the tide of dissent. LOMA granted the state extensive

surveillance powers through its intentionally vague language that “Any person who makes, publishes or communicates any statement...likely to cause fear, alarm and despondency...shall be guilty of an offence.”²⁶ The act permitted comprehensive surveillance of suspected individuals and organizations. It also allowed censorship of all publications and private correspondence, granted powers to restrict movement, assembly, and association. Additionally, search and seizure operations could be conducted without judicial oversight. The Emergency Powers Act (as amended in 1960) empowered the Smith administration to declare states of emergency, impose curfews and restrict movement, operate military tribunals, and authorise preventive detention without judicial review. From a surveillance perspective, it gave the government authority to monitor all forms of public assembly and communication as well as ban organisations and public gatherings. The Official Secrets Act (1970) banned disclosure of any matters “prejudicial to public safety.”

EARLY INDEPENDENCE PERIOD (1980-1990): CONTINUITY AND ADAPTATION

Upon independence in April 1980, the new ZANU-PF government under Robert Mugabe retained most colonial-era surveillance legislation. The Lancaster House Agreement’s protection of existing laws meant that instruments like the Official Secrets Act (1970) and LOMA (1960) remained in force, providing legal continuity for surveillance operations. A negotiated settlement, known as the Lancaster House Agreement of 1979, finally led to independence under majority rule the following year in April 1980. Robert Mugabe came in as the leader of the newly independent state which changed its name to Zimbabwe. As this and other sections will show, a change of leaders, a new name for the country and the advent of African

25 Britannica.com, Unilateral Declaration of Independence, <https://www.britannica.com/topic/Unilateral-Declaration-of-Independence>

26 National Archives UK, Law and Order (Maintenance) Act 1960 of Southern Rhodesia, <https://discovery.nationalarchives.gov.uk/details/r/C1194162>

majority rule did not lead to a rupture as the new regime retained most of the institutions, systems and laws of the colonial era.

The Official Secrets Act, Emergency Powers Act and LOMA and other colonial-era surveillance legislation, which had been the bane of African nationalist organisations and politicians like Mugabe, were retained and repurposed to fight erstwhile liberation allies-turned-foes like then opposition Zimbabwe African Peoples' Union (ZAPU) leader Joshua Nkomo and his followers. Over the course of Mugabe's long reign, which lasted until November 2017, the inherited laws were supplemented by new legislation and used to persecute civil society actors, members of the opposition, journalists, human rights defenders, ordinary citizens and anyone who was perceived a threat to the ruling elite. All this demonstrated how liberation movements inherited and perpetuated the very systems they once opposed as long as this suited their hegemonic interests rather than the democratic values they professed to uphold. This legal and institutional continuity with the colonial past was not accidental but a reflection of the new government's recognition of surveillance's utility for political control.

LOMA was given a new lease of life by the Mugabe regime and persisted to 2002. The retention of LOMA granted the state comprehensive surveillance powers through authorized surveillance of suspected persons without specific evidentiary requirements. It permitted interception of communications with minimal oversight and allowed preventive detention without trial. Additionally, it granted powers to restrict movement and assembly

The Emergency Powers Act was also retained in 1980. Section 3 stated that "During any period of public emergency, the President may make such regulations as appear to him to be necessary or expedient for securing the public safety, the defence of Zimbabwe, the maintenance of public order and the suppression of mutiny, rebellion and riot." This vaguely worded section gave the president so much discretion to pass measures which paved way to even greater surveillance against anyone on the pretext of national security. There was institutional continuity as the Mugabe regime retained the CIO and its Rhodesian era leadership. The spy agency was expanded to include more African operatives, mainly from Mugabe's Zanu party. The BSAP was renamed the Zimbabwe Republic Police (ZRP), and it inherited its predecessor's surveillance functions. Military intelligence remained central to political monitoring.

Rather than ushering in a new democratic dispensation, independence in 1980 simply marked a transfer of the coercive apparatus, laws, institutions and surveillance practices to the new regime. All these were used with devastating results by Mugabe as his administration presided over the massacres of 20,000 civilians in the Matabeleland and Midlands provinces.²⁷ The victims were targeted for allegedly supporting ZAPU. The killings, dubbed the Gukurahundi Genocide, were intelligence-driven.²⁸ Surveillance, infiltration, and data-gathering preceded and enabled the state violence, demonstrating how the colonial repressive doctrines were simply repurposed and deployed to serve postcolonial authoritarian consolidation.

27 Catholic Commission for Justice and Peace (1997). *Breaking the Silence, Building True Peace*.

28 The Gukurahundi genocide refers to the systematic massacre of over twenty thousand predominantly Ndebele speaking people in the Matabeleland and Midlands provinces in Zimbabwe from 1983 to 1987. The massacres were conducted by the Fifth Brigade of the Zimbabwean army. This unit, trained in North Korea, operated outside the regular military chain of command and reported directly to then Prime Minister Robert Mugabe. The violence stemmed from tensions between two revolutionary groups—the Zimbabwe African National Union—Patriotic Front (ZANU-PF), led by Mugabe, and the Zimbabwe African People's Union (ZAPU), led by Joshua Nkomo and it was primarily supported by Ndebele speaking people. <https://www.ebsco.com/research-starters/history/gukurahundi-genocide>; <https://davidcoltart.com/wp-content/uploads/2006/10/breakingthesilence.pdf>.

MUGABE IN THE 1990S: DEMOCRATIC OPENING AND SURVEILLANCE ADAPTATION

In the 1990s the regime faced growing opposition from civil society and political movements, culminating in the rise of the Movement for Democratic Change (MDC) party in 1999. Mugabe, who had arm-twisted Nkomo into dissolving his ZAPU party and agreeing for it to be absorbed by ZANU PF in the so-called Unity Accord of December 1987, still harboured hopes of establishing a one-party state. He responded to opposition by expanding and modernising the state's surveillance capabilities, combining the security apparatus and lawfare with informal intelligence networks. In addition to retaining colonial-era statutes such as the Official Secrets Act, LOMA and the Emergency Powers Act, the Mugabe administration consolidated rural surveillance networks through the enactment of the *Traditional Leaders Act* (1998).²⁹ This piece of legislation formally institutionalised the surveillance role of chiefs by requiring them to report on security matters, authorising them to collect intelligence within their jurisdictions, and obligating them to cooperate with state security agencies. The Act thus formalised the transformation of traditional authority structures into auxiliary arms of the security state. In doing so, Mugabe was not innovating but rather reviving colonial governance logics: successive settler administrations had similarly relied on African chiefs to surveil, discipline, and repress their subjects. What distinguished Mugabe's approach, however, was the juridical codification of this arrangement—embedding informal practices

of surveillance into enforceable law, thus extending the reach and legitimacy of the regime's security apparatus.

Throughout the 1980s, the Mugabe regime had relied on informal surveillance networks to augment the state security apparatus. These networks, which mainly operated in the rural areas, included chiefs, and Zanu PF party structures at cell, ward, district and provincial levels. When veterans of the 1970s guerrilla war of independence began pushing for gratuities, Mugabe responded with massive cash pay-outs and, more significantly, mobilising them to join the surveillance and security network..³⁰

The advent of the new millennium marked a pivotal and transformative phase in Zimbabwe's political trajectory. The formation of the Morgan Tsvangirai-led Movement for Democratic Change (MDC) in 1999 presented ZANU-PF with the most formidable opposition to its stranglehold on power since 1980. Faced with this existential threat, President Mugabe responded with a barrage of new laws aimed at entrenching surveillance and repression. Laws that would have regulated civic life in democratic societies were weaponised for state monitoring, curating dissent, and forestalling opposition. In many ways, this legislative turn echoed the authoritarian strategies of the colonial era, where LOMA and similar laws institutionalised surveillance as a means of quelling African nationalist mobilisation. Mugabe was thus drawing on the time-honoured colonial logics of control to build a surveillance strategy to deal with new political and civic threats to his rule in the 2000s.

The Broadcasting Services Act of 2001³¹ exemplified this continuity. Just like colonial authorities who had imposed restrictions on African newspapers, Mugabe's government sought to restrict the expanding media space and control the production and flow of information. The Act ensured state authority

29 International Labour Organisation, *Traditional Leaders Act* (No 25 of 1998) (Chapter 29), https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=57007

30 Wilfred Mhanda, *The role of War Veterans in Zimbabwe's Political and Economic Processes*, Solidarity Peace Trust, April 7 2011, <http://solidaritypeacetrust.org/1063/the-role-of-war-veterans/>

31 Law.co.zw, *Broadcast Services Amendment Act 2025 (Zimbabwe)*, Act No. 2 of 2025, <https://www.law.co.zw/download/broadcasting-services-amendment-act-2025-zimbabwe/>

over media houses by mandating them to acquire broadcasting licences and operate within a monitored system. The new law's content-monitoring provisions gave the state a legal basis to surveil programming and penalise broadcasters who deviated from state-approved narratives. In practice, this created an environment where only state-owned or Zanu-PF-aligned platforms such as the Zimbabwe Broadcasting Corporation (ZBC) could operate freely, ensuring a monopolisation of public discourse. The Act has been amended several times including in 2025, to accommodate digital-age reforms, including internet-based broadcasting, a revised board structure, and a new legal requirement for motorists to obtain a public broadcaster (ZBC) radio licence or exemption before getting a permit or insurance processing mandatory radio licensing for motorists.

Having silenced independent voices through the Broadcasting Services Act, the regime proceeded to extend its surveillance into political mobilisation through the passage of the Public Order and Security Act (POSA) 2002.³² Although this Act replaced the repealed colonial-era LOMA, it retained its predecessor's essential DNA. POSA granted the state sweeping powers to regulate and suppress public gatherings. Its clauses

empowered state authorities and the police bosses to determine whether opposition rallies, marches, or protests could be held. Thus,

constitutionally enshrined rights to assembly were turned into a privilege granted to the chosen ones by the regime. Political parties and civil society organisations now thus operated under severe legal restrictions, under constant surveillance and at risk of criminalisation.

POSA's colonial inheritance was clear: just like colonial administrators who had wielded 'public order' legislation against African political gatherings, framing them as potential sources of 'native unrest', Mugabe's POSA institutionalised suspicion of collective activity and legalised the treatment of democratic opposition as tantamount to criminal disorder.³³ In addition, it provided for the monitoring of civil society organisations and coordination between security services and informal surveillance networks

Not content with fashioning a noose around the necks of broadcasters, the Mugabe regime proceeded to impose restrictions against the press and all media practitioners in general through the heinous Access to Information and Protection of Privacy Act (AIPPA 2002).³⁴ This Act mandated all journalists to be registered with the Zimbabwe Media Commission (ZMC), which was established for the purpose.³⁵ As a result, journalism became a licensed profession, giving the state the ability to surveil journalists through their personal details and records embedded in state-held databases.

32 Veritas, "Public Order and Security Act [Chapter 11:17], as at 1st September 2016." Veritas. September 2016. <https://www.veritaszim.net/node/115>

33 Key Surveillance Provisions included Section 15: "A regulating authority may regulate, prohibit or impose conditions relating to the conduct of any public gathering if he considers on reasonable grounds that the gathering may result in... public disorder"; Section 16: Authorized comprehensive surveillance of political activities including the opposition; Section 24: Permitted surveillance and monitoring of all public gatherings; Section 30: Granted extensive powers to intercept communications during investigations

34 Veritas, Access to Information & Protection of Privacy

35 Surveillance Implications: Section 79: "No person shall practice journalism in Zimbabwe unless such person is registered in terms of this Act"; Section 15: Licensing requirements enabling comprehensive monitoring of media personnel; Section 20: Accreditation systems creating detailed databases of media practitioners; Section 25: Content restrictions facilitating censorship and surveillance of information flows

Through the Interception of Communications Act (ICA 2007) ³⁶the Mugabe administration advanced surveillance and repression further into the digital realm. The Act enabled direct state intrusion and access to telephone, electronic, and internet communications. A government minister, rather than an independent court, was empowered to issue surveillance warrants, creating a unilateral executive arbiter for intrusion into private life. All this was done ostensibly in the name of national security, which in Zimbabwe, as in Rhodesia, was just a byword for the protection of the ruling elite. Telecommunications providers were compelled to install interception technologies and retain subscriber data, a move that effectively integrated private firms into the state surveillance apparatus.³⁷ In addition to political opposition, civil society actors and ordinary people, circumstances may arise where the target of surveillance is either a journalist and or lawyer. The Act is silent on how such surveillance should be carried in respect of these two professions whose members' rights are both guaranteed and protected under the constitution and common law.

With this Act Mugabe demonstrated that he had learnt everything and forgotten nothing from the successive colonial regimes whose institutions and practices he had vowed to dismantle before he assumed the reins of power. Where colonial regimes had relied on informants, postal censorship, and police dossiers, Mugabe's ICA recalibrated these practices into the age of fibre networks, mobile telephony, and digital archives.

Old-fashioned surveillance practices had been spruced up and given new legal robes suitable for the digital era of the 21st century.

The regime instituted several informal Surveillance Networks to extend their reach. One was the National Youth Service (NYS). Popularly known as Green Bombers because of their green training uniform, the NYS was established as a youth militia in 2001 by the now deceased Youth minister and Zanu PF legislator, Border Gezi.³⁸ Their Surveillance Functions included community-level intelligence gathering and reporting; Monitoring of opposition party activities in rural areas; Enforcement of political conformity through violence and intimidation; Coordination with formal security services during elections; Surveillance of international NGO and donor activities. As early as January 2002, army sources confirmed that while the director of the National Youth Service, David Munyoro, was a civilian, the unit was at that time run by a military man, retired Brigadier Boniface Hurungudu. This demonstrated the formal military coordination with informal surveillance networks.

In addition to this was the Joint Operations Command (JOC). ³⁹The JOC has its roots in the Rhodesian Security Forces and was established during the liberation struggle, as the Combined Operations Headquarters. It was set up in to coordinate Rhodesia's counter-insurgency campaign. The organisation was retained and revived to coordinate the new government's response to internal and external security threats after independence. The JOC is a powerful

36 Zimlil. "Interception of Communications Act Chapter 11:20." Zimlil, June 10, 2025

37 Key Surveillance Provisions: Section 5: Authority to intercept all telephone communications; Section 8: Powers to monitor internet and electronic communications; Section 12: Access to postal and courier services; Section 15: Real-time monitoring capabilities for security services; Section 18: Data retention requirements for service providers

38 CSVR, Fear, Terror and the Spoils of Power: Youth Militias in Zimbabwe, March 1, 2005, <https://www.csvr.org.za/fear-terror-and-the-spoils-of-power-youth-militias-in-zimbabwe/#:~:text=The%20national%20youth%20training%20was,August%202001%20with%201000%20recruits.>

39 Enock Ndawana and Fritz Nganje, Militarisation and State Capacity in Zimbabwe: The Limits of the Human Security Paradigm, Global Society, Volume 38, 2024, Issue 2, August 17, 2023, <https://www.tandfonline.com/doi/abs/10.1080/13600826.2023.2246504#:~:text=As%20a%20result%2C%20the%20JOC,the%20economy%2C%20elections%20and%20politics.>

body that brings together the heads of all of Zimbabwe's security services, including the military, police, and intelligence agencies. Its role is to oversee and coordinate national security, although it has accused of playing a significant role in political and electoral processes in the country including surveillance. JOC represents the integration of formal and informal surveillance capabilities: Coordination between CIO, military intelligence, and police; Integration of informal surveillance networks into formal operations; Joint planning of electoral surveillance and intimidation campaigns; Unified command structure for surveillance operations.

Taken cumulatively, the Broadcasting Services Act, POSA, AIPPA, and ICA ensured that Zimbabwe's laws legitimised authoritarian consolidation at the expense of democracy and civil rights. ZANU–PF thus demonstrated that it did not believe in reactive and ad hoc censorship, but it had embraced a layered system of surveillance encompassing every aspect of public life, including speech, assembly, journalism, and communications. Licensing requirements converted routine bureaucratic compliance into opportunities and occasions for surveillance. Political contestation and public gatherings were reframed as security risks, inviting infiltration and monitoring. Far from being independent actors, journalists were reclassified as licensed subjects whose legitimacy depended on submission to the state. Telecommunications lost their status as a secure realm of private exchanges and free flow of ideas; they were transformed into open highways of state intrusion.

Laws not only legitimised and rationalised repression, they also gave it an appearance of normalcy, dressing surveillance in the language of order, information management, and above all, national security. Perhaps the most significant aspect of these laws of the latter Mugabe era is that they laid the foundation for Zimbabwe's progression into

the fully-fledged surveillance state that it has become under his successor, President Mnangagwa.

THE MNANGAGWA ERA (2017–PRESENT): THE DIGITAL SURVEILLANCE STATE

Since seizing power in 2017, President Mnangagwa's regime unleashed Zimbabwe's most systematic campaign of repression—weaponising laws, state machinery and private entities against dissenters with unprecedented scope and technological sophistication.

President Mnangagwa and his supporters market his ascension to power as the dawn of the Second Republic in Zimbabwe. They like to call it a democratic rebirth, but this is merely Orwellian doublespeak which masks a dark reality that under his watch, Zimbabwe has been transformed into a digital panopticon where surveillance predicts and crushes dissent before it emerges. Where Mugabe built the scaffolding of authoritarian control, Mnangagwa has engineered a technologically enhanced surveillance apparatus that monitors, anticipates, and neutralises threats in real-time.

Under Mnangagwa, Zimbabwe has crossed the proverbial Rubicon from analogue to algorithmic authoritarianism. Surveillance is no longer reactive—it is predictive, pre-emptive, and designed to strangle opposition in its womb. Thus, with Mnangagwa at the helm, Zimbabwe has made a quantum and qualitative leap in authoritarian governance: from monitoring dissent to forecasting and preventing it entirely.

This is not surprising given that Mnangagwa is a disciple of Mugabe. Having been close to Mugabe since 1977, initially as his personal assistant, Mnangagwa became Zimbabwe's founding State Security minister and self-proclaimed “Godfather” of the CIO.⁴⁰ He boasts that nothing could happen in Zimbabwe

40 The NewsHawks, Mnangagwa boasts of being “CIO Godfather”, November 21, 2023, <https://thenewshawks.com/mnangagwa-boasts-of-being-cio-godfather/>

without his knowledge because he was responsible for the reconfiguration of the CIO after independence. Mnangagwa was in the thick of security matters in the early 1980s, playing a critical role in the intelligence-driven Gukurahundi massacres where 20 000 civilians were massacred in Zimbabwe's Matabeleland and Midlands provinces. The massacres were part of the Mugabe regime's methods of neutralising the Joshua Nkomo-led opposition ZAPU party which drew most of its support from those provinces.⁴¹

Declassified South African documents from the 1980s reveal a telling irony. While Mugabe publicly condemned Apartheid in South Africa, Mnangagwa was secretly meeting with South African intelligence operatives, apparently seeking methods to eliminate real and perceived security threats to their respective countries. At that time, Apartheid South Africa was under the stewardship of hardline Prime Minister Pieter Botha. Botha and Mnangagwa shared the moniker "Crocodile"—but for Mnangagwa, those who know him say the nickname captures not guerrilla heroics, but predatory cunning and calculated ruthlessness. Mugabe even warned Zimbabweans that Mnangagwa was unforgiving and always went after his perceived enemies.⁴² In line with Mugabe's warning, Mnangagwa has clamped down on the opposition, human rights defenders, civil

society and journalists using repressive laws and surveillance.⁴³ The clampdown has often led to killings.⁴⁴

Mnangagwa has overseen a legal recalibration that fuses continuity with the colonial and Mugabe eras with digital authoritarian innovation. The Cybersecurity and Data Protection Act of 2021 marks Zimbabwe's formal entry into and codification of digital-age surveillance—legitimising state intrusion under the guise of promoting cybersecurity.⁴⁵ It provides for the establishment of a state-controlled Cybersecurity Centre housed in the Office of the President, merging cybersecurity with interception of communications. It mandates data retention by service providers, authorises real-time monitoring of internet activity, and grants intelligence services broad access to personal data. Despite the façade of "data protection," the Act codifies executive control over digital surveillance.⁴⁶

Rather than safeguarding citizens' data, this Act systematically dismantles privacy rights through provisions which establish comprehensive surveillance capabilities. Three following provisions reveal the true intentions of the state: Section 35 allows broad national security exceptions to data protection; Section 40 authorises broad intelligence service access to personal data;

41 Jeffrey Moyo, Anger resides decades after 1980s genocide in Zimbabwe, Anadolu Anjisi, August 1, 2021, <https://www.aa.com.tr/en/africa/anger-resides-decades-after-1980s-genocide-in-zimbabwe/2320958#:~:text=Current%20leaders%20responsible%20for%20genocide,in%20an%20estimated%20%2C000%20deaths>

42 Xaxa, Mnangagwa does not forgive anyone says Mugabe, Pindula Online, March 21, 2018, <https://news.pindula.co.zw/2018/03/21/mnangagwa-does-not-forgive-anyone-says-mugabe/>

43 Human Rights Watch, Zimbabwe Events of 2022, <https://www.hrw.org/world-report/2023/country-chapters/zimbabwe#:~:text=The%20human%20rights%20climate%20in,committed%20by%20state%20security%20forces.>

44 US State Department, 2023 Country Report on Human Rights Practices: Zimbabwe, <https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/zimbabwe#:~:text=Significant%20human%20rights%20issues%20included,problems%20with%20the%20independence%20of>

45 Veritas, Cyber and Data Protection Act (Chapter 12:07) (No 5 of 2021, <https://www.veritaszim.net/node/5522>

46 Key Sections: Section 10: "A law enforcement agent may, with a warrant issued by a magistrate, access any computer system or data for the purpose of investigating any offence"; Section 15: Authority to monitor all internet communications; Section 20: Data retention requirements for all service providers; Section 25: Government access to personal data for security purposes; Section 30: Cybercrime investigation powers including real-time monitoring

and Section 45 authorises international intelligence sharing agreements without any safeguards or oversight.

The Cybersecurity and Data Protection Act is designed to regulate the processing of personal information and enhance cybersecurity. The Act's title promises cybersecurity and data protection, yet its substance delivers the opposite. By deliberately conflating cybersecurity with national security, the Mnangagwa regime has created legal justification for sweeping surveillance powers. As the Media Institute of Southern Africa (MISA-Zimbabwe) notes, this false equation serves authoritarian purposes: cybersecurity affects all internet users, but treating it as national security transforms every citizen into a potential threat.⁴⁷

The Act establishes the Cybersecurity and Monitoring of Interception of Communications Centre—a surveillance apparatus that consolidates unprecedented power within the Office of the President. This institutional design—according to MISA—eliminates checks and balances by placing the same entity responsible for monitoring communications in charge of authorising that monitoring. The result is systematic targeting of political opponents without judicial oversight. The Centre operates with an expansive mandate that includes monopolising all authorized interceptions, implementing government cybercrime policy without independent oversight, and identifying “intervention areas” for cybercrime prevention—language broad enough to encompass virtually any digital activity.

Section 164 exemplifies how the Act weaponises vague language against

journalistic freedom. Citizens face five years imprisonment or maximum fines for transmitting data messages deemed to “incite violence”—a standard so subjective that even legitimate reporting is criminalised. The case of journalist Blessed Mhlanga demonstrates this danger; he was charged with inciting violence in February 2025. His supposed crime was broadcasting his interview with ruling Zanu-PF party Central Committee member and war veteran Blessed Geza, who viciously attacked President Mnangagwa for alleged corruption and gross violations of the constitution, and demanded his ouster. Mhlanga was charged with allegedly “inciting violence”. His case was investigated not just by the regular police, but by its Counter-Terrorism Unit — a frightening development that reveals the Zimbabwean regime’s conflation of journalism with terrorism.⁴⁸

This criminalisation of journalism most likely represents a deliberate state strategy of promising rights while simultaneously criminalising their exercise. The Act even establishes a whistleblower protection system, yet operates within a framework that treats dissent as potential criminality.

FROM LOMA TO POSA TO THE MAINTENANCE OF PEACE AND ORDER ACT, 2019

From 1980 to 2002 the draconian Law and Order Maintenance Act (LOMA), which was inherited from the Rhodesian government, was one of the primary laws used for surveillance, especially monitoring citizens in public places.⁴⁹ Enacted in 1960, Loma was replaced by the Public Order Maintenance Act (Posa)⁵⁰ in 2002, although the new Act

47 Misa Zimbabwe, “Analysis of the Data Protection Act.” Misa Zimbabwe, December 6, 2021. <https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/>.

48 Amnesty International, Zimbabwe: The Arbitrary Detention of Journalist a Brazen Attack on Press Freedom, Amnesty International, 2025, <https://www.amnesty.org.zw/2025/02/zimbabwe-the-arbitrary-detention-of-journalist-a-brazen-attack-on-press-freedom/>.

49 Troicare, The Zimbabwean Struggle: Obstacles to Democracy, Troicare, 2004, <http://archive.niza.nl/docs/200407081448317449.pdf>.

50 Veritas, “Public Order and Security Act [Chapter 11:17], as at 1st September 2016.” Veritas. September 2016. <https://www.veritaszim.net/node/115>

retained about 90% of LOMA's draconian provisions.⁵¹ Between 2002 and 2019, POSA became the centrepiece for State sanctioned repression because it granted broad and repressive powers to the government and security forces to monitor, restrict, and suppress dissent and opposition. POSA was used to disrupt civil society activities such as workshops and public debates, effectively monitoring and controlling political and social discourse. It empowered security agents to monitor public gatherings and demonstrations as well as to prohibit them. The security forces were given authority to arrest, detain and use force to suppress "unlawful" demonstrations.

In 2019, the Mnangagwa administration repealed POSA and enacted the Maintenance of Peace and Order Act (MOPA). Although it was touted as progressive legislation, MOPA preserves core surveillance capabilities while expanding police powers to monitor and control public gatherings and movements to maintain public order and security.⁵² The Act regulates public processions, demonstrations and meetings. It makes it mandatory for the police to be given notice, allowing police to appoint conveners and authorised officers to oversee gatherings. Police have powers to disperse gatherings and take steps to prevent disorder or damage. The Act allows the police to demand identity documents to enable them to identify and track individuals during surveillance operations, and makes it mandatory for citizens to carry identity cards. Police are granted sweeping powers to disperse assemblies and prevent what they deem "disorder"—language vague and broad enough to encompass virtually any unwanted political expression.

Most concerning are the Act's warrantless search provisions. Police officers can stop and search any person, vehicle, or vessel without judicial authorisation if a senior officer decides such action is necessary for "public safety, order or health." This standard is so subjective it effectively eliminates constitutional protections against unreasonable searches. The law also empowers police to establish security cordons around areas experiencing "public disorder" and conduct searches for suspects or evidence without warrants. Combined with mandatory identity card requirements, these provisions enable systematic tracking and harassment of citizens.

The controversial Private Voluntary Organisations Amendment (PVO) Bill was signed into law by President Mnangagwa on 11 April 2025 ushering in yet another massive hurdle in the fight for civic space in Zimbabwe.⁵³ The new law introduces significant amendments to the PVO Act, Money Laundering and Proceeds of Crime Act, and Criminal Law Act, making it easier for the government to monitor civil society organisations and activists.

The act imposes strict governmental oversight of non-governmental organisations (NGOs), scrutinising their operations and funding while criminalising non-compliance. It gives the state unfettered powers to snoop into operations of civic society organisations (CSOs), trusts and other humanitarian organisations, who are now expected to hand over sensitive personal data to the government. In addition, it threatens civic space and making it difficult for NGOs to operate without state interference.⁵⁴

51 Paul Kaseke, "Posa is that you – Part 1." NewsDay, April 30, 2019. <https://www.newsday.co.zw/columnists/article/56742/posa-is-that-you-8211-part-1>

52 Veritas, "Maintenance of Peace and Order Act (MOPA)", Veritas, 2019, https://www.veritaszim.net/sites/veritas_d/files/Maintenance%20of%20Peace%20&%20Order%20Act.pdf.

53 Veritas. "BILL WATCH 12-2025 of 22nd April 2025 [The PVO Amendment Act- Validity Questioned]." Veritas, 2025. <https://www.veritaszim.net/node/7440>

54 Makumbe, C. T. "Regulation Or Repression? The Divisive Impact Of Zimbabwe's PVO Amendment Bill." NGO AfricaWatch, April 11, 2025. <https://ngoafriwatch.net/2025/04/11/regulation-or-repression-the-divisive-impact-of-zimbabwes-pvo-amendment-bill/>.

Key Provisions include Mandatory Registration and Stringent Reporting where all PVOs are now required to register with the Registrar's Office. The Bill allows the Registrar to demand comprehensive information regarding the organisations' governance, beneficial ownership, and funding channels. PVOs that are currently operating as trusts and associations would immediately be rendered unlawful if they continue to operate and receive donations from the public or donations from sources that are outside the country. 'Restrictions on Political Activities' is one of the Bill's most contentious clauses which prohibits PVOs from engaging in any form of political lobbying. Critics argue that the definition of "political activity" is overly broad and could stifle legitimate advocacy and civic education. Government representatives assert that these restrictions are necessary to prevent politically motivated misappropriation of resources.

The Bill also consolidates significant power in the hands of the Registrar and, indirectly, the Minister of Justice, Legal and Parliamentary Affairs. It grants these authorities the discretion to designate a PVO as "high risk" should its funding or activities raise concerns about potential links to terrorism or money laundering. In such cases, the Bill enables intervention measures that could include suspension, deregistration, or replacement of leadership. The Minister has wide discretionary powers which could be used to interfere with the operations of NGOs. He can suspend the executive committee of an organisation and replace it with a provisional trustee/s who can make far reaching changes in the organisation. A Minister can also suspend and disqualify individuals from holding office without giving them an opportunity to be heard.

Peter Mutasa, the Crisis in Zimbabwe Coalition (CiZC) director, was highly critical of the passage of the Act. CiZC is a conglomerate of more than 80 influential

Zimbabwean CSOs. "It (the passage of the Act) is a sad development. It is shameful, that Zimbabwe a country borne out of a bitter but courageous struggle for freedom and democracy has joined apartheid South Africa and colonial Rhodesia in taking away citizens' rights and freedoms. Mugabe, in all his brutality, did not assent to this type of law," Mutasa said in 2022 when the Act was passed.

In April 2025, the Postal and Telecommunications Regulatory Authority of Zimbabwe (Potraz) announced plans for mandatory registration of all mobile devices, linking SIM cards to biometric and personal data. Potraz justified the move on the grounds of bolstering national security and combatting cybercrime.⁵⁵ However, the proposal has torched a storm with critics arguing that this will only increase privacy invasion and bolster state surveillance operations, as it requires users to submit personal data as part of the registration requirements.

Taken together, Zimbabwe's legislative framework under President Mnangagwa operates across the following multiple domains to create a comprehensive surveillance state:

Digital Surveillance: The Cybersecurity Act centralises all electronic monitoring within the Office of the President, eliminating judicial oversight while criminalising legitimate journalism and political expression.

Physical Surveillance: MOPA authorises warrantless searches, mandatory identification requirements, and comprehensive monitoring of public gatherings and movement.

Legal Intimidation: deliberately vague and subjective standards for "incitement," "public disorder," and "cybercrime" establish broad discretionary powers that can be weaponised against any form of dissent.

55 Oluchukwu Ikemefuna, "Zimbabwe's Telecom Regulator, POTRAZ Wants to Track All Mobile Phones in an Effort to Combat Cybercrime," Silicon Africa, April 14 2025, <https://silicon africa.org/potraz-wants-to-track-all-mobile-phones-to-combat-cybercrime/>.

Institutional Capture: By housing surveillance capabilities within the office of the president and the executive branch while eliminating

independent oversight, the system ensures that monitoring serves political rather than security purposes.

THE SURVEILLANCE APPARATUS: THE CIO, THE ARMY AND THE POLICE

The contemporary Zimbabwean surveillance state operates through a tripartite institutional structure encompassing military intelligence (Zimbabwe Defence Forces- ZDF), civilian intelligence (CIO), and law enforcement agencies (Zimbabwe Republic Police- ZRP).

These are all coordinated through the Joint Operations Command (JOC) rather than the constitutional National Security Council. This arrangement bypasses civilian oversight and concentrates surveillance powers within security apparatus loyal to the ZANU-PF party leadership.

Surveillance in Zimbabwe dates back to the colonial era, when the Rhodesian government built a security and intelligence system to suppress African nationalist movements. This network included the Rhodesian Army, the British South Africa Police (BSAP) and the Special Branch, which specialised in intelligence work. The Special Branch later became part of the Central Intelligence Organisation (CIO) which was created in 1963. Special Branch stations were established in most of the larger towns throughout the provinces.⁵⁶ The Branch infiltrated liberation movements, monitoring political activities and compiling detailed records on nationalist leaders. It relied heavily on a broad network of

informants, including coerced collaborators in rural areas and worked closely with the army to identify insurgents.

The Selous Scouts, an elite counter-insurgency unit formed in 1973, were infamous for pseudo-operations in which they posed as guerrillas to infiltrate and dismantle liberation groups. Their missions included deep-penetration surveillance, cross-border raids into Zambia and Mozambique, and targeted assassinations, often relying on intelligence extracted through torture and interrogation.⁵⁷

The Rhodesian Army's Military Intelligence Branch collaborated with the BSAP and Special Branch, collecting operational intelligence for counter-insurgency campaigns. This included aerial reconnaissance, signals interception, and deploying reconnaissance units along borders. These efforts aimed to track the movement of liberation fighters, map infiltration routes, and prevent attacks on key targets.⁵⁸

56 Bsapolice.org, Force Branches, <https://www.bsapolice.org/thematic/force-branches/>

57 Pamusoroi.com, The Selous Scouts (ca. 1977), November 23, 2020, <https://pamusoroi.com/history/selous-scouts>

58 Selous Scouts and counter-insurgency methods Selous Scouts / "Rhodesian operations; overview sources on pseudo-operations and human intelligence practices" October 2005. CDL PubISS Africa

At independence, these surveillance methods, legal frameworks and the doctrines underpinning them were not dismantled but simply repurposed and adopted by the reconstituted army (ZDF), police (ZRP) and intelligence (CIO) to serve the hegemonic interests of the ruling ZANU-PF elite⁵⁹

MILITARY SURVEILLANCE IN THE MNANGAGWA ERA

The ZDF, particularly through its military intelligence unit—the Zimbabwe Intelligence Corps (ZIC)—has long been a key player in domestic surveillance operations. In 2020, then army commander Edzai Chimonyo publicly stated that the army would begin monitoring social media activity as part of national security measures. That same year, there were media reports of large-scale deployments of ZIC officers, alongside members of the elite Special Air Service (SAS) and the Special Investigations Branch (SIB), into communities nationwide. Military sources told the local *Zimbabwe Independent* newspaper that the troops had been embedded in the communities to gauge ZANU-PF support and Mnangagwa's popularity. This strategy reflected state anxiety over growing political unrest amid economic decline, illustrating how surveillance intensifies during periods of instability.

Reports from human rights organisations, including the NGO Forum, indicate that the military also employs advanced surveillance technology to spy on political activists, journalists, and human rights defenders. Forum.⁶⁰ As a core member of the Joint Operations Command (JOC), the army has considerable influence over internal

security and along with the police and CIO, it is not subjected to any oversight- a task which ought to be performed by the non-operational National Security Council. Intelligence training programmes equip army officers with sophisticated eavesdropping and electronic monitoring capabilities, signalling the institutionalisation of mass surveillance.

Historically, the military's involvement in domestic politics has been overt and coercive. A striking example occurred during the 2008 presidential elections when the army intervened to reverse Robert Mugabe's electoral defeat to Morgan Tsvangirai in the first round of voting. The military effectively overthrew the electoral process and unleashed violence and intimidation on a wide scale, ahead of the runoff prompting Tsvangirai to withdraw and leave Mugabe to contest alone.⁶¹ Tsvangirai's opposition MDC party alleged that at least 500 of its members were killed during that election.⁶²

THE CIO: COVERT SURVEILLANCE

The CIO operates Zimbabwe's most sophisticated and extensive intelligence infrastructure, integrating physical tracking, infiltration, and communications interception. Its operatives frequently infiltrate opposition parties, activist movements, and civil society organisations, while maintaining broad authority to monitor communications (telephone calls, text messages and internet communications) under the Interception of Communications Act. This law compels telecommunications providers to maintain subscriber databases accessible to the CIO and other security agencies, ostensibly to

59 "Academic analysis of institutional continuity and the security sector's political role Oxford/academic reviews on military in politics and continuity' October 2005. [Oxford Research EncyclopediaORA](#)

60 NGO Forum, "Communications and Political Intelligence Surveillance on Human Rights Defenders in Zimbabwe". Zimbabwe National NGO Forum. https://www.hrforumzim.org/wp-content/uploads/2024/11/BPUK15104_Insides.pdf

61 Chris McGreal, "This is no election. This is a brutal war." The Guardian, June 22, 2008. <https://www.theguardian.com/world/2008/jun/22/zimbabwe1>

62 VOA, "Zimbabwe's Former Opposition MDC Says 500 Died In 2008 Political Violence." Voice of America, August 9, 2009. <https://www.voanews.com/a/a-13-2009-08-09-voa21-68705422/409301.html>

safeguard national security but in practice enabling pervasive state surveillance.⁶³

The CIO's partisan political role was evident during the 2023 general elections, when it assumed control of election-related security operations through Forever Associates Zimbabwe (FAZ), an organisation led by CIO deputy director-general, retired Brigadier-General Walter Tapfumaneyi. The spy agency has also been implicated in numerous abductions, enforced disappearances, and extrajudicial killings under both the Mugabe and Mnangagwa administrations. The March 2015 abduction of activist Itai Dzamara remains one of the most prominent unresolved cases, emblematic of the agency's use of surveillance and terror to silence dissent.

THE ZRP: SURVEILLANCE THROUGH POLICING

Under President Mnangagwa, the ZRP has expanded its surveillance functions through the Internal Security Intelligence Unit to monitor social media platforms, WhatsApp groups, and mine CCTV footage. During protests in March 2025, over 100 activists were arrested based on evidence from Harare's citywide surveillance network, illustrating the operational integration of technology into policing. Police also arrested administrators of WhatsApp groups linked to protests. In rural and urban settings alike, the police have established informant networks under the guise of neighbourhood watch programmes, reinforcing the state's capacity for grassroots intelligence gathering. Surveillance vans equipped with recording equipment frequently appear at demonstrations, serving as both monitoring tools and psychological deterrents.

Draconian laws such as the Maintenance of Peace and Order Act (MOPA) continue to legitimise surveillance and repression.

Opposition figures, particularly former Citizens Coalition for Change (CCC) leader Nelson Chamisa, have repeatedly denounced the police for systematically disrupting their rallies—reporting over 62 cancelled events in under a year. In a rare internal rebuke, senior police officials in 2023 issued directives urging officers to stop banning opposition rallies, reflecting growing scrutiny of police practices ahead of elections.⁶⁴

INFORMAL SURVEILLANCE AND SOCIAL PENETRATION

Mnangagwa has revived informal surveillance actors, embedding the state within communities. In 2021 he revived the National Youth Service (that was originally launched in August 2001). Explaining the move, prominent Zimbabwean scholar, Professor Martin Rupiya, states, “amid the intense political struggle between the ruling party and a largely worker- and urban-society-based political opposition, there was an urgent need to have in place a cheap and available institution that could be relied upon both to toe the party line religiously and to execute state supported extra-legal activities, including violence. The institution, drawn from the country's earlier political history, the Zimbabwe Peoples' Militia, now reincarnated as the National Youth Service (NYS).” After being neglected for many years post 2005, the Mnangagwa regime resolved to revive the Service, ostensibly to instil a sense of patriotism in young people. However, critics argue that just as it was in 2001, the rationale remains unchanged. They argue the government only wants to create a youth militia to execute the state and ZANU-PF's hegemonic agenda by conducting community-level intelligence gathering and social media monitoring, among other things.

The president also revived the Community Policing Forums. These so-called

63 Zenzele Ndebele, “Zimbabwe enacts phone tapping law.” Anadolu Ajansi, October 2, 2013. <https://www.aa.com.tr/en/world/zimbabwe-enacts-phone-tapping-law/214320>

64 Kennedy Nyavaya, “Stop banning opposition rallies: Police chiefs order station officers.” Newsday, July 10, 2023. <https://www.newsday.co.zw/local-news/article/200013806/stop-banning-opposition-rallies-police-chiefs-order-station-officers>

neighbourhood watch committees sometimes play a dual role of fighting crime in their areas and conducting surveillance, which can be used for political ends. They have, in some instances, been turned into reporting networks feeding intelligence to the police. Traditional Leaders (Chiefs and village headmen) have been incentivised through state patronage to serve similar purposes. Lavished with vehicles and money, they function as political intelligence conduits in rural areas. They have a long history of helping mobilise villagers within their jurisdictions to vote for ZANU-PF as well as intimidating those who side with the opposition. These informal actors extend surveillance into the social fabric, ensuring that communities monitor themselves in a climate of mutual suspicion.

SURVEILLANCE TECHNOLOGY AND PRACTICES IN THE MNANGAGWA ERA

Despite being rooted in colonial legacies and post-independence authoritarianism, the Mnangagwa regime has increasingly invested in advanced surveillance technologies to enhance its control mechanisms. While early surveillance primarily depended on informants, intelligence networks, and rudimentary tracking methods, contemporary operations utilise sophisticated digital monitoring capabilities, often facilitated by foreign technological partnerships with external enablers, particularly Chinese and Israeli firms.

Authorities actively track social media activity to identify critics and suppress dissent. The Cyber Security and Data Protection Act (2021) provides the legal basis for monitoring online communications. Government agencies reportedly use software to scan

platforms like Facebook, X (formerly Twitter), and WhatsApp for 'subversive' content. Activists and journalists have been arrested on account of social media posts deemed critical of the state. For instance, in 2020, the now deceased army commander, Edzai Chimomyo, said the army would snoop into private communications to 'guard against subversion', signalling Zimbabwe's transition towards a comprehensive surveillance state.⁶⁵ In March 2025, the ruling ZANU-PF claimed it had developed sophisticated systems to track individuals using anonymous profiles on social media. The party's Secretary for Legal Affairs Patrick Chinamasa also claimed they could expose "ghost accounts" responsible for cyber-bullying.⁶⁶ These developments represent a systematic approach to digital control that extends beyond passive monitoring to active identification and targeting of individuals engaging in online political discourse.

Zimbabwe's telecommunications infrastructure serves as a conduit for state surveillance activities of phone Tracking and interception. The absence of robust legal protections against surveillance, as noted by the MISA, creates an environment where the Interception of Communications Act (2007) enables extensive surveillance without adequate oversight mechanisms. Telecommunications companies are legally required to integrate interception technologies, including deep packet inspection (DPI) and International Mobile Subscriber Identity (IMSI) catchers, enabling real-time monitoring capabilities, which are often misused to target dissenters.⁶⁷ The government has found it even easier to track down citizens, with mobile networks collecting real-time location data from cell towers. Authorities have used such data to trace the movements of activists, as seen in

65 Brenna Matendere, "Army to monitor social media," *Newsday* (Harare), March 3, 2020, <https://www.newsday.co.zw/slider/article/48340/army-to-monitor-social-media>.

66 Tinashe Ngoro, "ZANU PF Has Developed Technology To Unmask 'Ghost' Accounts On Social Media: Chinamasa," *iHarare*, March 7 2024, <https://iharare.com/zanu-pf-has-developed-technology-to-unmask-ghost-accounts-on-social-media-chinamasa/>.

67 MISA Zimbabwe, "Surveillance and privacy," MISA Zimbabwe (Harare), 2020, <https://zimbabwe.misa.org/issues-we-address/surveillance-and-privacy/>.

cases where protesters were arrested based on their proximity to demonstrations in 2020.

Evidence suggests systematic data collection by the government from mobile network providers without the knowledge and consent of the user, with the opposition and human rights defenders being the primary targets. For instance, opposition Citizens Coalition for Change legislator Joana Mamombe, along with Netsai Marova and Cecilia Chimhiri, were tracked through their mobile devices before being arrested and subsequently abducted from police custody in May 2020. They were tortured and sexually assaulted after leading an anti-government protest.⁶⁸ The trio successfully petitioned the High Court to order Zimbabwe's largest telecommunications provider, Econet Wireless, to release cell phone records of their movements on the day they were abducted to prove that they had indeed been kidnapped by state security agents.⁶⁹

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) also facilitates state access to users' comprehensive telecommunications data, including call records, SMS logs, and internet usage patterns. This system extends beyond security applications to social control mechanisms, as evidenced by the government's use of algorithmic analysis of telecommunications data for aid distribution in 2020. At the time, Finance Minister Mthuli Ncube revealed that algorithms would analyse bank accounts, mobile wallets, and location data to determine aid eligibility, illustrating how surveillance infrastructure permeates multiple aspects of civic life.

However, the data collection was done without consent.⁷⁰ Since 2013, Zimbabwe has enforced mandatory SIM card registration, which requires users to submit national identity details. While officially justified as a security measure to combat crime, this system creates comprehensive databases linking phone activity directly to individuals, facilitating targeted surveillance of persons of interest.

The government has already begun moves to instal surveillance cameras at checkpoints and major cities. In August 2024, the Bulawayo City partnered with South African company, Tendy Three Investments (TTI), to roll out Chinese made close-circuit television (CCTV) cameras to monitor both pedestrian and vehicle traffic in the city.⁷¹ Digital rights activists and experts worry that the footage could be used by the state to clamp down on dissent, particularly during street protests. In 2018, the Mnangagwa administration introduced biometric systems for voter registration and national identification, marking a significant expansion of state surveillance capabilities. While framed as security enhancement measures, these systems enable mass data collection and potential political profiling of citizens. In addition, the government has embarked on a Cyber City development project in Mt. Hampden on the outskirts of the capital, Harare. The envisaged city will incorporate comprehensive biometric surveillance systems but critics have pointed out that the project could lead to the institutionalisation of surveillance infrastructure within urban planning and development frameworks in Zimbabwe. Critics have also expressed

68 Amnesty International, "Abducted, beaten, sexually assaulted and jailed for protesting," Amnesty International Zimbabwe (Harare), 2021, <https://www.amnesty.org/en/petition/abducted-beaten-sexually-assaulted-and-jailed-for-protesting/>.

69 Pellargia Mupurwa, "High Court orders Econet to release GPS data in MDC activists abduction saga." September 3, 2020. <https://techmag.tv/2020/09/03/high-court-orders-econet-to-release-gps-data-in-mdc-activists-abduction-saga/>

70 Farai Mudzingwa, "Mthuli Ncube & His 'Sophisticated Algorithms' For Corona Relief Funds – Another Privacy Disaster Looming?," TechZim (Harare), 2020, <https://www.techzim.co.zw/2020/04/mthuli-ncube-his-sophisticated-algorithms-for-corona-relief-funds-another-privacy-disaster-looming/>.

71 <https://cite.org.zw/big-brother-is-watching-tti-installs-street-cameras-on-cbd-roads/> accessed on 27 August 2025

concern that facial recognition systems installed as part of the project could be used by the state to identify and suppress

dissenting voices in a country known for police brutality, unlawful arrests and detentions.⁷²

FOREIGN ENABLERS OF SURVEILLANCE

Zimbabwe has undergone a rapid transformation into a comprehensive surveillance state under President Mnangagwa's administration, facilitated by strategic partnerships with external actors, particularly Israel and China.

This section examines how external technology transfers and capacity-building initiatives have enabled the rapid deployment of sophisticated monitoring infrastructure that extends far beyond traditional security applications into comprehensive social control mechanisms.

ISRAEL

In 2021, Misa Zimbabwe wrote to the parliament of Zimbabwe expressing concern over the acquisition of surveillance spyware by the state. This followed credible reports that Zimbabwe is a customer of Israeli telecom company, Circles, a surveillance firm that produces technology with capabilities of exploiting weaknesses in the global mobile phone system to snoop on calls, texts, and the location of phones around the world⁷³. Circles exploits flaws in Signalling System—the set of protocols that allows networks to exchange calls and text messages. This allows government agencies to track individuals across borders without a warrant, bypassing international conventions. Circles

was found to have been used in the 2019 internet shutdown, following fuel protests in Zimbabwe. Circles is reportedly affiliated with NSO Group, which develops the often-abused Pegasus spyware, that can infiltrate smartphones, extract messages, photos, emails, and even activate microphones and cameras without the user's knowledge.⁷⁴ Misa said it was concerned about the use of such tools in the absence of substantive cybersecurity and data protection legislation in Zimbabwe. The media advocacy body also criticised the lack of transparency around the acquisition of this cybersecurity equipment and the conditions under which it is sold to Zimbabwe. Zimbabwe is one of several countries that have been using Israeli spyware, according to a 2021 report by *The Middle East Monitor*⁷⁵. Another report by the University of Toronto's Citizen Lab revealed that government agencies in Zimbabwe, Botswana, Equatorial Guinea, Kenya, Morocco, Nigeria and Zambia are using the surveillance technology developed by Circles to spy on the personal communications of opposition politicians, human rights activists and

⁷² Ayang MacDonald, "Zimbabwe govt faces criticism over biometric surveillance project for new smart city," Biometric Update, February 28, 2023. <https://www.biometricupdate.com/202302/zimbabwe-govt-faces-criticism-over-biometric-surveillance-project-for-new-smart-city>.

⁷³ Misa Zimbabwe, "Concern over acquisition and use of surveillance tools in Zimbabwe," Misa Zimbabwe, 2021

⁷⁴ David Pegg and Sam Cutler, "What is Pegasus spyware and how does it hack phones?" The Guardian, 2021.

⁷⁵ The Middle East Monitor, "African governments are crushing opposition using Israeli spyware," The Middle East Monitor, 2021

journalists.⁷⁶ In its investigations, *Citizen Lab* detected three Circles platforms, with one dating back to 2013. A second platform was activated in March 2018 and is still operating.

The spyware was also used by Zimbabwe's CIO to record disgraced Vice-President Kembo Mohadi's sordid calls and messages to a harem of women — some of them married — in a sensational sex scandal which shook the corridors of power in Harare (Gagare 2021)⁷⁷. Audios of Mohadi's calls were subsequently leaked on social media platforms, in what analysts believed was linked to infighting within the ruling ZANU PF. The Middle East Monitor also reported that surveillance conducted via the Circles spyware facilitated a government crackdown on anyone exposing corruption. Investigative journalist Hopewell Chin'ono, and opposition politician Jacob Ngarivhume, were both arrested and detained ahead of planned anti-government protests in 2020.

The most damaging Israeli-linked company operating in Zimbabwe has been Nikuv. Over the years, Nikuv International Projects, an Israel-based private company whose beneficial owners have links to the Israeli intelligence agency, Mossad, has played a key role in surveillance and alleged vote rigging in Zimbabwe. The firm has courted controversy in several other African countries including Angola. It has close links with fellow Israeli company, International Security Council which is staffed by former Mossad officials,⁷⁸ which has prompted speculation that Nikuv could be a front for Mossad.

Nikuv specialises in population registration, election systems, identity cards, and passports. It was established in 1994 and is a subsidiary of the Formula Group, one of Israel's largest software groups. The company operates internationally, primarily in governmental sectors across African countries including Zimbabwe, Zambia, Ghana, Botswana, Lesotho and Angola. Widespread reports indicate that Nikuv has been active in Zimbabwe since the 1990s and it allegedly manipulated the voters roll and helped rig the 2008 and 2013 elections to ensure former President Mugabe and his ZANU- PF party retained power. The Israeli company has operated hand in glove with Zimbabwe's security apparatus, allegedly collaborating closely with the military and CIO in election rigging while also helping the Zimbabwe police to acquire supplies as part of sanctions-busting measures.

While Nikuv has maintained a low profile in recent years in Zimbabwe; its subsidiary Pedstock, remains operational, supplying various agricultural equipment and technology. Pedstock was implicated in a money laundering operation before it was subsequently revealed that the firm was helping the Zimbabwean government to pay another Israeli company, Glamer Limited, for secret work that the latter had done for the Zimbabwean government and the police.⁷⁹ Pedstock was also involved in Zimbabwe's command agriculture- a failed nationwide army-run scheme aimed at boosting food security. The scheme is alleged to have been a conduit for the looting of billions in US

⁷⁶ Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis and Ron Deibert, "Running in Circles – Uncovering the Clients of Cyberespionage Firm Circles," *Citizen Lab*, December 1, 2020

⁷⁷ Owen Gagare, "Zim uses Israeli spying technology to snoop on citizens' calls, messages," *The NewsHawks*, 2021

⁷⁸ Sam Sole, "'Zim voters' roll in hands of suspect Israeli company'," *Mail and Guardian*, April 12, 2013 <https://mg.co.za/article/2013-04-12-zim-voters-roll-in-hands-of-suspect-israeli-company/>

⁷⁹ Charles Laiton, "Secret payments to Nikuv exposed", *The Standard*, May 19, 2019, <https://www.thestandard.co.zw/2019/05/19/secret-payments-nikuv-exposed>

dollars from state coffers. In 2019, officials from Zimbabwe's Agriculture ministry told Parliament's public accounts committee that they had no idea how US\$2,9 billion disbursed for command agriculture was utilised.⁸⁰ That same year, Pedstock was summoned by Zimbabwe's parliament to explain how it spent about US\$7 million allocated to it under the Command Agriculture scheme.⁸¹ Pedstock had been granted US\$6,907,927 to supply irrigation equipment to farmers under the government's subsidised inputs programme during the 2018/19 agricultural season.

Nikuv also reportedly infiltrated opposition circles through Pedstock. The agricultural company installed agricultural equipment for senior opposition figures, including Morgan Tsvangirai well ahead of the 2013 elections and the opposition were not aware of Pedstock's links to Nikuv.⁸² Pedstock supplied and installed drip irrigation systems at Tsvangirai's rural home in Buhera, before extending similar services to other opposition leaders. Other beneficiaries were former MDC vice-president Thokozani Khupe and Tsvangirai's chief secretary, Ian Makone and his wife, Theresa, who was Home Affairs minister in a 'government of national unity' with ZANU PF from 2009 to July 2013. This access to senior opposition leaders created surveillance opportunities which were probably exploited by ZANU PF and the security agencies. Pedstock still operates in Zimbabwe and it is one of the major suppliers of high-end irrigation equipment and technology.

NIKUV AND ELECTION RIGGING

According to confidential documents, Nikuv first established ties with Zimbabwe in November 1994, signing a US\$15 million

contract to computerise the Ministry of Home Affairs, the census office, and the electoral system.⁸³ The deal was backed by Israel's Foreign Trade Risks Insurance Corporation. In addition to providing technological support, Nikuv, through various subsidiary companies, played a major role in assisting the Zimbabwean police to circumvent international sanctions and procure riot control equipment and motorbikes from a company linked to Nikuv, Beit Alpha. The equipment was purchased ahead of the 2002 presidential elections. A Dutch registered company Pedfora linked to a brother of Nikuv's founder, Emmanuel Antebi, also clandestinely purchased quad bikes for Zimbabwe's police without going to tender.

Confidential state documents also reveal that Nikuv was rehired in November 2007 for a six-month period ahead of Zimbabwe's 2008 elections. It was tasked with computerising all identity documents for use in the voters' roll, a service for which it was reportedly paid US\$7.6 million. A Zimbabwean Home Affairs Ministry official was quoted in a confidential document, stating that that: "The Israelis were the major force in controlling the (2008) elections process, especially with regard to the counting and announcement of results."

Prior to the elections, Nikuv had already been mentioned in rigging plots because of its role in compiling the voters' roll which was stuffed with ghost voters. An analysis by the opposition MDC found that some voters were registered at addresses with no residential structures. It was further alleged that Nikuv had assisted ZANU-PF in restricting opposition access to the voters' roll, which the opposition had sought to use for targeted campaigning.⁸⁴ An information technology

80 Obey Manayiti and Rutendo Matanhike, "Mnangagwa ally faces probe in 3bn scandal," The Standard, July 21, 2019 <https://www.newsday.co.zw/the-standard/2019/07/21/mnangagwa-ally-faces-probe-3bn-scandal>

81 Philemon Jambaya, "Parliament summons Nikuv over Command Agriculture," Nehanda Radio, October 20, 2019, <https://nehandaradio.com/2019/10/20/parliament-summons-nikuv-over-command-agriculture/>

82 Mail & Guardian, "MDC's naïve Nikuv dealings", August 16, 2013, <https://mg.co.za/article/2013-08-16-00-mdcs-naive-nikuv-dealings/>

83 Guardian and Sun, "Inside the P200m spy tender," Guardian and Sun, April 11, 2013, <https://guardiansun.co.bw/News/inside-the-p200m-spy-tender>

84 Mandy Rossouw, "Israeli spooks paid to clinch Mugabe win," Mail and Guardian, 2008

expert, Valentine Sinemane, subsequently stated that the electronic version of the voters' roll, sold to the opposition by the Zimbabwe Electoral Commission (ZEC) was compiled by Nikuv and stuffed with ghost voters.

During the 2008 elections, *The Zimbabwean*—an independent weekly newspaper—reported that 20 Israelis arrived as government guests to bolster President Mugabe's election-rigging efforts. They were reportedly met by senior members of CIO and taken to a secure location in Harare to meet with ZEC officials.⁸⁵ ZEC took more than five weeks to announce 2008 presidential election results, way longer than the five days it normally takes for the results to be announced. When the results eventually came out, the official ZEC count gave opposition politician Morgan Tsvangirai 47.9% of the vote while Mugabe supposedly garnered 43%. This meant that none of the candidates had obtained the required 50.1% to be declared winner, hence a runoff was declared. The opposition and Tsvangirai himself believed that he had comfortably surpassed the threshold and accused Zanu PF and Nikuv of rigging.

Liberation stalwart and long-serving former ZANU-PF secretary for administration Didymus Mutasa, who at one time served as Minister in Mugabe's office in charge of the CIO, later confirmed that Tsvangirai had indeed won the elections. Mutasa, who was expelled from ZANU-PF after falling out with

then President Mugabe over succession issues, even offered to provide proof to the opposition MDC or appear as a witness in court should the party seek his help.⁸⁶

Nikuv courted even greater controversy in Zimbabwe's 2013 elections when it resisted calls to release the final voters' roll, only doing so on polling day. This was criticised by Southern African Development (SADC) election observers who stated that "a voters' roll should not be a top-secret document".⁸⁷ The *Zimbabwe Independent* reported that Nikuv founder and chief executive, Emmanuel Antebi arrived in Zimbabwe a day before the 2013 elections to meet Mugabe and other senior Zanu PF officials allegedly to finalise the deal to engineer the results.⁸⁸ Ahead of the 2013 elections, Nikuv operated from the Registrar General's offices in Harare, where it was also involved in civil registration, particularly passport production. The firm received payments in excess of US\$10 million from the Registrar General's office between February and July 2013 and it was subsequently awarded a new tender to take complete charge of Zimbabwe's passport printing. This was seen as a reward for facilitating the rigging of elections in favour of ZANU PF.⁸⁹ In the aftermath of the 2013 polls, Tsvangirai supplied the constitutional court with a dossier showing over 50 payments to Nikuv as part of his ultimately unsuccessful case to overturn Zanu PF's 'victory'.⁹⁰ Nikuv subsequently relocated data files from its old offices at the Registrar General's offices to new premises at the army headquarters in

85 Cambridge Forecast, "Israel helping the ruling parties in an African country to rig elections," Cambridge Forecast, April 10, 2008, <https://cambridgeforecast.wordpress.com/2008/04/10/mugabe-zimbabwe-israel/>

86 Stephen Jacks, "Mutasa ready to expose NIKUV scam", Bulawayo 24, June 23, 2015, https://bulawayo24.com/index-id-news-sc-national-byo-69877.html#google_vignette

87 Brenna Matendere, "Zec not fit to hold free, fair and credible 2023 elections," The NewsHawks, February 26, 2023, <https://thenewshawks.com/zec-not-fit-to-hold-free-fair-and-credible-2023-elections/>

88 Elias Mambo, "Zimbabwe: Israeli Agents Rig Results," August 2, 2013, <https://allafrica.com/stories/201308020997.html>

89 Bulawayo 24, "Nikuv rewarded with new project", Bulawayo 24, December 6, 2013, <https://bulawayo24.com/index-id-news-sc-national-byo-39869.html>

90 Wonai Masvingise and Moses Matenga, "Zim Elections: 'Nikuv paid \$10 million to rig'," NewsDay, August 10 2013, <https://www.newsday.co.zw/politics/article/163971/zim-elections-nikuv-paid-10-million-to-rig>.

Harare and this demonstrated its close links with the security agencies.⁹¹

CHINESE COMPANIES AND THEIR ROLE IN SURVEILLANCE

Huawei and ZTE are two of major Chinese telecommunications giants that have supplied Zimbabwe with network infrastructure incorporating comprehensive surveillance capabilities. Reports suggest that these companies have provided voice and data interception systems integrated into mobile networks. Huawei has also secured several major contracts with the Zimbabwean government and state-owned entities like Net-One, the country's second largest Mobile Network Operator.⁹² Huawei supplied the mobile communications equipment that has been rolled out nation-wide by Net-One. Concerns around the security of Huawei's communication equipment have seen the US leading a call for the banning and phasing out of the use of Huawei telecommunications equipment. Other countries such as Britain, Australia and New Zealand have taken steps to remove or block Huawei from their 5G rollouts due to widespread fears that the firm's equipment is embedded with capabilities to conduct surveillance on behalf of China. However, Zimbabwe has no such qualms. If anything, the use of Huawei and other Chinese-sourced equipment is likely to expand following a controversial government directive to the country's mobile network

operators to enter into infrastructure sharing agreements. Additionally, Chinese firms have enhanced the Zimbabwean government's surveillance capabilities by building the National Data Centre which consolidates citizens' data for ease of access. Zimbabwe has also deployed facial-recognition systems supplied by Chinese biometric firms like CloudWalk, integrating them into CCTV networks at ports of entry and selected urban hubs. These deployments have been presented to government as "smart city" or "security modernisation" projects.⁹³

LOCAL TELECOMMUNICATIONS COMPANIES AND ELECTIONS

The Zimbabwean government has also faced criticism for accessing and using data held by mobile communications service providers to gain political mileage for ZANU-PF. Ahead of both the 2018 and 2023 elections, mobile communications subscribers received personalised political messages from ZANU-PF, a clear indication that the party had access to citizens' data, which it could potentially abuse for even more sinister ends.⁹⁴ Econet was accused of handing over subscribers' data to ZANU-PF without their consent, charges which the telecommunications operator denied. Regardless of who the culprit was, the episodes demonstrated that subscribers are not safe from the prying eyes of the surveillance state.

91 Elias Mambo, "Nikuv moves data files to KGVl," The Zimbabwe Independent, 2014

92 Tapiwa Mapigoti, "Huawei and Surveillance in Zimbabwe," Privacy International (London), 2021, <https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe>.

93 Ron Deibert et al., "Running in Circles: Uncovering the Clients of Cyberespionage Firm, Circles," The Citizen Lab, University of Toronto, December 1, 2020. The Citizen Lab

94 Leonard Chaparadza, "ZANU-PF Sending Personalised Messages To Individuals, Where Did They Get That Database? Electoral Commission and Econet Says Not From Them," TechZim July 9, 2018. <https://www.techzim.co.zw/2018/07/econet-denies-selling-customers-data-to-3rd-parties-refutes-zecs-allegations-so-who-sold-data-to-zanu-pf/>.

SURVEILLANCE AND ITS IMPACT ON ELECTIONS AND DEMOCRACY IN ZIMBABWE

While surveillance has always played a big part in deciding election outcomes in favour of ZANU-PF, at no time has it been deployed as comprehensively as in the 2023 polls elections when the CIO unleashed Forever Associates Zimbabwe (FAZ)- a pseudo civic organisation to coordinate surveillance operations extending from national to grassroots levels.

FAZ was headed by then CIO deputy director general, Retired Brigadier General Walter Tapfumaneyi, who was shunted back to the army and rewarded with a promotion to major general most likely as a reward for his contributions to ZANU-PF's disputed electoral triumph.

An investigation by *The NewsHawks* revealed that FAZ was deeply involved in election preparations and it had spread its tentacles to every ward in the country, collecting vital voters' details right down to household level using an army of 5 910 information gatherers.⁹⁵ The information gatherers — three in each of the country's 1 970 wards — worked under the close supervision of their CIO handlers. FAZ officials were seen conducting door to door visits in both urban and rural areas, causing discomfort among voters. They had ZANU-PF membership records but also visited opposition supporters' homes, as part of a recruitment and intimidation campaign. The CIO strategy enabled the ruling party to control the electoral process in terms of structures, numbers of registered voters and the actual voting process, as well as polling stations. It also promoted systematic voter intimidation and victimisation, especially at ward level.

An operational FAZ document titled *FAZ Campaign Scope*, revealed that the shadowy organisation had penetrated all provinces up to household level through several tactics, leaving voters vulnerable to abuse during the election period. "FAZ volunteers are required to intrusively access party cell registers, from party cell chairmen, and check and verify their accuracy and integrity. To this end, FAZ then discretely conducts a head count of cell members, checking if they are registered to vote. If any party members or holders of positions of leadership are found not to have national documents or registered to vote, FAZ, therefore, will handhold and assist all those to rectify the discrepancy under supervision," the document reads.⁹⁶

Critical information collected by the agents and informers included names, addresses, identity numbers and voter registration details at polling station level. FAZ also counted people at household level before recording the information on their tablets and smartphones.

The information was computed, condensed into data and processed to enable the influencing and manipulation of the electoral process in favour of ZANU-PF through a combination of tactics, including

95 Morris Bishi, "CIO-linked outfit takes over ahead of watershed elections," *The NewsHawks*, 2023, <https://thenewshawks.com/cio-linked-outfit-takes-over-ahead-of-watershed-elections/>.

96 The document was accessed by our researcher. No copy was ever published although another organisation later also wrote about it. <https://thesentry.org/wp-content/uploads/2024/05/ForeverAssociatesZimbabwe-May2024-TheSentry.pdf>

persuasion and, in some cases, intimidation. The data was also used to predict potential outcomes, giving ZANU-PF a clear idea of the constituencies and wards where it needed to deploy more campaign resources or activate its feared coercive machinery. Various civil society organisations including Human Rights Watch⁹⁷ and several observer missions like SADC⁹⁸ and the European Union (EU)⁹⁹ condemned FAZ's role in the polls.

While FAZ was given a free reign to manipulate the election outcome, independent election monitoring groups were persecuted as evidenced by the arrest of 39 staffers of the Zimbabwe Elections Support Network (ZESN) as well as the Elections Resource Centre. The police confiscated laptops, cell phones and other communication gadgets as part of pre-emptive moves to stop the independent election monitoring groups from conducting parallel election tabulation.¹⁰⁰ Comprehensive surveillance systems had enabled the police to learn of the organisations' plans for a parallel vote tabulation process- something not proscribed by law. It is widely believed that the polls were rigged just like many others before them, including the 2013 and 2018 elections.

The 2000, 2002, 2005 and 2008 elections were also accompanied by widespread violence, which was mostly preceded by surveillance

of opposition officials and supporters. A 2009 Human Rights Watch indicates that at least 163 people were killed while 5000 were tortured or beaten in the 2008 election runoff. Perpetrators included the police, military, police and ZANU -PF officials who acted with absolute impunity.¹⁰¹ Surveillance was reported on a wide scale, while torture, mutilations and killings of victims across the country were also reported. For example, a staunch MDC-T activist Tonderai Ndira was brutally murdered by state agents who had tracked him to his Harare residence just two weeks after presidential election results were announced.¹⁰² The trauma of his killing continues to haunt his family and his widow no longer attends political rallies and refrains from any involvement in electoral activities.¹⁰³

Eight years earlier, ZESN's Political Violence Monitoring Subcommittee recorded 31 killings, 70 abductions and 500 cases of severe injuries in the run up to the 2000 elections.¹⁰⁴ The organisation also reported that ZANU PF-aligned independence war veterans encamped on more than 1 600 farms with a farm worker population of over 400 000 around the country. The illegal farm occupations allowed for wide scale intimidation and targeted violence against potential voters. More than 2 400 cases of violence were recorded, leading to the hospitalisation of 400 farmers and workers. At least 1 500 death threats were also recorded during that period.

97 <https://www.hrw.org/report/2023/08/03/crush-them-lice/repression-civil-and-political-rights-ahead-zimbabwes-august-2023> accessed on 27 August 2025

98 <https://www.newzimbabwe.com/zimbabwe-elections-observer-missions-raise-concern-over-faz-as-govt-defends-the-shadowy-zanu-pf-affiliate/> accessed on 27 August 2025

99 <https://www.zimlive.com/eu-final-report-fingers-zec-judiciary-faz-for-aiding-mnangagwa-poll-victory/> accessed on 27 August 2025

100 ZimLive, "Police raid 2 election organisations, arrest 39 to stop parallel vote tabulation," ZimLive, 2023, <https://www.zimlive.com/police-raid-2-election-organisations-arrest-39-to-stop-parallel-vote-tabulation/>.

101 Human Rights Watch, "Zimbabwe events of 2008," Human Rights Watch, 2009, <https://www.hrw.org/world-report/2009/country-chapters/zimbabwe>.

102 Daniel Howden and Raymond Whitaker, "Murdered by Mugabe's mob," The Independent UK, 2008, <https://www.independent.co.uk/news/world/africa/murdered-by-mugabe-s-mob-838145.html>.

103 Ruvimbo Muchenje, "Ndira's widow carries heavy heart," The NewsHawks, May 31, 2023. <https://thenewshawks.com/ndiras-widow-carries-heavy-heart/>

104 Zimbabwe Election Support Network (ZESN), "Report On The 2000 Parliamentary Elections Zimbabwe," Zimbabwe Election Support Network, 2000, <https://www.zesn.org.zw/wp-content/uploads/2015/10/ZESN-Report-on-the-2000-Parliamentary-Elections.pdf>.

Linda Masarira, leader of the opposition Labour, Economists and African Democrats (LEAD) who was barred from contesting the 2023 presidential elections after the Nomination Court rejected her papers, says pervasive surveillance and violence have instilled deep fear among citizens, leaving many powerless to speak out or challenge the repressive state. She said a cocktail of repressive laws, relentless surveillance, and political violence has forced opposition parties and civil society into survival mode, crippling their ability to campaign, organise rallies, or engage in robust policy debate. “In Zimbabwe’s context, surveillance is not about national security. It’s about regime security. It is a deliberate strategy to stifle democratic space and keep the ruling elite entrenched. The state has created an Orwellian system where surveillance is pervasive, opaque, and unaccountable, resulting in gross violations of human rights, including the rights to privacy, freedom of assembly, freedom of expression, and the right to participate in public affairs.”¹⁰⁵

“Ultimately, surveillance in Zimbabwe has crippled democracy, reducing elections to ceremonial exercises marked by intimidation and coercion. We are now living in a surveillance state where free thought and expression are policed, punished, and suppressed. For democracy to thrive, surveillance must be subjected to strict oversight and transparency in alignment with constitutional rights and international human rights standards,” Masarira said in an interview. Masarira spent three months in pre-trial detention after being arrested for participating in nationwide public protests dubbed *#ShutdownZim2016* in July 2016. Like many other politicians and activists, Masarira’s arrest was preceded by and facilitated by police intelligence reports after monitoring social media and surveillance footage.¹⁰⁶

OPPOSITION POLITICIANS’ EXPERIENCES OF SURVEILLANCE-ENABLED PERSECUTION

Like Tsvangirai, Chamisa, Masarira and many others, veteran opposition politician Job Sikhala has been endured so much surveillance-enabled persecution dating back to his student activism days in 1996. He has been arrested and detained on numerous occasions and his most recent stint was a 595 day stay in remand prison before being freed in January 2024. Recounting his experiences, Sikhala recently told Intelwatch repression had intensified over the years as the ZANU-PF government increased its spending particularly on technology to enhance its surveillance capabilities.¹⁰⁷ “There is round-the-clock physical surveillance of individuals,” Sikhala said.

“They also use technology to snoop in on private conversations by hacking WhatsApp and emails of the opponents of the regime. They also deploy informers and their agents around your house. They have done this to me on several occasions, often using my neighbours’ houses as centres for monitoring my movements to establish the times I leave my house and when I return,” Sikhala said, adding the surveillance and resultant persecution extended to his family and friends. Far from being advancing national security interest, Sikhala said surveillance was merely a tool for regime survival and it had resulted in the violation of constitutionally guaranteed freedoms of movement and expression among other rights.

Opposition Transform Zimbabwe party leader Jacob Ngarivhume has also endured surveillance-enabled arrests and detention over the course of his political life. Ngarivhume spent eight months in jail on accusations of inciting public violence.

¹⁰⁵ Interview with Linda Masarira, Harare 2025

¹⁰⁶ Ross, Booty, and Nyoka, Zimbabwe Police Arrest Dozens in Wake of Protests, BBC, 1 April 2025, <https://www.bbc.com/news/articles/czx4g9ejjj9o>

¹⁰⁷ Idah Nassah, “Zimbabwe Opposition Leader Freed After 595 Days Behind Bars,” Human Rights Watch, 2024, <https://www.hrw.org/news/2024/01/31/zimbabwe-opposition-leader-freed-after-595-days-behind-bars>.

This followed his call for a peaceful protest against poor governance by the Mnangagwa regime in 2020. Harare magistrate Feresi Chakanyuka sentenced him to four years in jail in April 2023 but the High Court quashed the conviction on appeal.¹⁰⁸ In 2024 he spent 82 days in prison after being arrested for participating in a gathering allegedly meant to incite public violence.¹⁰⁹

He recently told Intelwatch that the surveillance and persecution extended to his wife and primary school-going children. “I have been under a lot of surveillance from the state apparatus. I’m used to them roaming the streets near my home. I’m used to them following my car. I’m used to all that. My children in primary school also know that cars follow them. It brings huge pressure,” Ngarivhume said. He added that surveillance had deleterious effects on democracy as it was deterring people from actively participating in politics.

The surveillance state operates with such impunity that abductions occur in broad daylight. On 1 November 2023, opposition Citizens Coalition for Change (CCC) legislator Takudzwa Ngadziore was tracked while travelling to parliament and kidnapped by state agents. Ngadziore managed to livestream his capture on Facebook as he fled into what appeared to be a garage, pursued by two rifle-wielding men. No action was ever taken despite the viral video and the subsequent identification of his captors as Central Intelligence Organisation (CIO) operatives.¹¹⁰

Ngadziore was found hours later, dumped naked in Mazowe, some 20 kilometers from Harare and rescued by artisanal miners who provided clothing. He subsequently sued the government for his abduction. The

psychological and social impact extends far beyond physical trauma—Ngadziore recently told Intelwatch that surveillance and torture affected his family’s mental health while making him “a social misfit” as friends and colleagues feared association would expose them to danger.

Ngadziore’s testimony reveals the extent of the deeply damaging effects of the surveillance.¹¹¹ “State surveillance is a tactic used by the regime to silence dissent. When someone holds contrary opinions toward the socio-economic or political narrative they’re pushing, they utilise surveillance and this often leads to abductions, torture, or state-sponsored violence. I’ve been a victim of such oppressive methods by the state to silence dissent. I was abducted on 1 November 2023, while traveling to Parliament, tortured with iron bars and electric implements, and dumped in Christon Bank (Mazowe), on a mountain. (In the interrogation), the questions focused on my criticism of government actions and reactions in the political sphere. This torture affects not only the body but psychological well-being—you lose your mental equilibrium. I spent months in hospital and had to take a parliamentary break. My parents felt it wasn’t safe for me to continue activism or human rights work. And the experience also takes away the friends that you have and turns you into a social pariah. In that regard will limit who you associate and interact with. Other people feel you expose them to danger merely by your presence. The regime uses this strategy believing people will be silenced, but it only strengthens one’s resolve.

We’ve witnessed the abduction and torture of many activists who speak truth to power, accompanied by unjust arrests on flimsy charges—another method the regime uses

108 Voice of America (VOA), “High Court Acquits Jailed Zimbabwe Opposition Leader,” Voice of America, 2023, <https://www.voazimbabwe.com/a/high-court-acquits-jailed-zimbabwe-opposition-leader-/7392967.html>.

109 Zimbabwe Lawyers for Human Rights (ZLHR), “Ngarivhume Set Free after 82-Day Detention,” Zimbabwe Lawyers for Human Rights, 2024, <https://www.zlhr.org.zw/?p=3346>.

110 Zimlive, “CCC MP Ngadziore abductors unmasked,” ZimLive, November 2, 2023. <https://www.zimlive.com/ccc-mp-ngadziore-abductors-unmasked/>

111 Interview with this author

to silence dissent. When you're followed by unidentified vehicles or individuals, you face harm, danger, and violence. This demonstrates the regime's intolerance toward different perspectives. Their lack of tolerance pushes them to conclude that silencing dissenting voices is the only way to control democratic space. We've seen the victimization arrests of Makomborero Haruzivishe, Namatai, Joanna Mamombe, and Cecilia Chimhiri—people vocal about political issues in our country. These experiences are devastating because they reveal our democracy as a sinking ship, tagging our nation as an authoritarian and totalitarian regime where people cannot express their views without being tortured. The tactics utilised by the regime are something that we totally condemn. I've sought professional help to recover from mental trauma. Torture destroys your ability to trust anyone or coexist peacefully in society, knowing you're safe. The fear intensifies because I was injected with an unknown substance, meaning any health issue makes you wonder if it's connected to your torture experience. For any democratic society to treat citizens this way—when the state should be a parent to its citizens—is beyond unfair. It's unjust and excruciatingly sad.”

SURVEILLANCE AND ITS IMPACT ON HUMAN RIGHTS DEFENDERS

Human Rights Defenders (HRDs) in Zimbabwe, particularly those who are vocal or influential in the public sphere, often face threats to their lives. State security agents meticulously track their activities, closely monitoring their locations and engagements. This surveillance empowers state agents to disrupt meetings and protests and to intimidate dissenters, instilling fear to suppress any voices that could challenge

the government's propaganda. Over the years, security agents have ruthlessly cracked down on demonstrations. In some cases activists are arrested ahead of planned demonstrations. In January 2019, for example, Zimbabweans took it to the streets to demonstrate against a 150% fuel price hike announced by President Mnangagwa. The protest lasted three days but security forces fired live ammunition at unarmed protesters, killing 17 people.¹¹² Human rights organisations reported that some women were raped. A year later, in May 2020, Mnangagwa publicly disparaged activists, branding protests as “political grandstanding” during a speech at the burial of ZANU-PF official Absalom Sikhosana.

False accusations are also being weaponized. The chilling effects of such rhetoric are evident, as activists are often forcibly taken from their homes, subsequently enduring torture and abuse, only to be vilified and framed as criminals. The case of opposition legislator Joanna Mamombe and activists Cecilia Chimhiri and Netsai Marova illustrates this systematic approach. On 13 May, 2020, the trio were arrested at a roadblock while returning from a demonstration in Harare's Warren Park suburb. They had been protesting the government's failure to provide essential food supplies during COVID-19 lockdown.¹¹³ The three women were subsequently abducted from the police station by unidentified men driving a black Toyota Wish. They were tortured and sexually assaulted over two nights after being forced into a pit. They were later dumped near Bindura.

Despite visible evidence of their ordeal, authorities arrested the victims while they were hospitalised, charging them with “communicating falsehoods” and “faking their abduction.” Police never explained why they

112 Human Rights Watch, “Zimbabwe: Excessive Force Used Against Protestors,” Human Rights Watch, March 12, 2019. <https://www.hrw.org/news/2019/03/12/zimbabwe-excessive-force-used-against-protesters>

113 Amnesty International, “Tortured activists released on bail,” Amnesty International, 2020. <https://www.amnesty.org.uk/urgent-actions/tortured-activists-released-bail>

initially confirmed arresting the three women, only to reverse their statement the following day. Marova later fled into exile leaving Mamombe and Chimbiri to face a lengthy trial before they were acquitted in July 2023.¹¹⁴

In another case of surveillance-led persecution, activists, Robson Chere, Namatai Kwekweza, Samuel Gwenzi and Vusumuzi Moyo were tracked to Robert Mugabe International Airport in Harare and abducted from a plane before it took off for the Victoria Falls on 31 July 2024.¹¹⁵ They were on their way to the 5th African Philanthropic Conference, an annual gathering of civil society policy influencers and other stakeholders. They were charged with disorderly conduct allegedly for participating in a demonstration against the detention of opposition Citizens Coalition for Change (CCC) politician Jameson Timba and 78 party activists at the Harare Magistrates' Court. Timba and his co-accused had themselves been arrested during a private meeting at the former's home. They faced bizarre charges of unlawful gathering and disorderly conduct, despite that theirs had been a private meeting at Timba's home.

Chere and fellow activists' treatment reveal the torture apparatus underlying Zimbabwe's surveillance state. Chere arrived in court bloodstained and barely able to walk. Lawyers argued that their clients were abducted from the aircraft and tortured for hours before being delivered to police. In his court testimony, Chere revealed that his captors threatened to kill him or rape his wife if demonstrations occurred during the SADC summit Zimbabwe was due to host that year.

Most chillingly, the abductors demonstrated their surveillance capabilities by telling Chere

precisely where his wife and children were located at that moment, emphasising their vulnerability.¹¹⁶ Kwekweza, who had been out of the country when the alleged protests occurred, had a booted foot shoved into her mouth. They also forced a metal bar into her mouth even though they were well aware that she was recovering from a recent dental procedure. Moyo endured prolonged interrogation by different people who demanded details about his income sources and ordered him to warn CCC politicians Ostallos Siziba and Takudzwa Ngadziore against organising demonstrations.

The year 2019 will forever be etched in Amalgamated Rural Teachers Union of Zimbabwe leader Obert Masaraure's memory, for painful reasons. Masaraure was abducted twice in six months and on both occasions he was tortured by state security agents. "I have been abducted twice by the Zimbabwean state. The first instance was on 18 January 2019. The second was on 5 June 2019," he said in an interview with Intelwatch. The First Abduction occurred in 18 January 2019 during the time of fuel price hike protests. Armed men broke into Masaraure's home at night. When he investigated noise outside his bedroom, he encountered AK47-wielding assailants in his corridor who immediately grabbed and beat him with rifle butts. Most disturbingly, this torture occurred in front of his wife and children in their own home.

"When my children emerged screaming, they bundled me into a vehicle and drove to an unknown location where the torture continued," Masaraure recalls. "They (assailants) later received a phone call and dumped me at Harare Central Police Station around 3am." The state accused Masaraure of

114 NewZimbabwe, "Abduction trial, CCC's Mamombe, Chimbiri off the hook acquitted on communicating falsehoods charges," July 5, 2023, <https://www.newzimbabwe.com/abduction-trial-cccs-mamombe-chimbiri-off-the-hook-acquitted-on-communicating-falsehoods-charges/>

115 SRDefenders, "Zimbabwe: enforced disappearance, cruel treatment, arbitrary detention and judicial prosecution of Namatai kwekweza." SRDefenders, October 21, 2024. <https://srdefenders.org/zimbabwe-enforced-disappearance-cruel-treatment-arbitrary-detention-and-judicial-prosecution-of-namatai-kwekweza-robson-chere-and-samuel-gwenzi-joint-communication/>

116 Zimlive, "Families of jailed rights defenders threatened, court told of torture horror." ZimLive, August 3, 2024.

organizing the fuel protests that left several people dead as demonstrators took to the streets of Harare and Bulawayo, using burning tires to barricade roads after President Mnangagwa's 150% fuel price increase aimed at addressing shortages and "rampant" illegal trading.

The Second Abduction occurred six months later on the 5 June 2019. "We had organised a protest demanding better wages for teachers. It was a three-day protest starting from the third of June to the fifth. On the final night of the strike action, armed men broke into our house," he said. "I managed to hide, but when they couldn't find me, they threatened to torture my wife. I emerged to protect her. They forced me into a white Fortuner and drove to a destination I couldn't recognise in the darkness."

At what later emerged as a bushy area near Manyame military base, Masaraure endured severe torture. "They forced me to remove all clothing, then beat me with sjamboks while forcing me to roll in mud they'd created by pouring water. When I was nearly unconscious, they left me naked after taking my clothes, money, and cell phones." He said his family's phones were also confiscated to prevent contact. In winter's cold, Masaraure had to find his way home naked. He eventually encountered a woman who coincidentally had previous experience helping tortured victims—suggesting the area served as a regular torture and dumping ground near Manyame Barracks. She provided warm clothing and transport money to return home.

The psychological impact extends far beyond the immediate victim. Masaraure says his eldest son, now 13, was most severely affected. He was eight years old when he witnessed the abduction. "The traumatic experience left a permanent mark on my family. I remember being called to my eldest sons school. I was told he consistently told teachers that he hated people in uniforms, he despised police officers and military officers," Masaraure said, adding his wife was also affected. "Even my wife had to seek counselling. It was a problem because we

struggled to sleep at home because any noise at night made us fear their return. The traumatic experience left permanent marks on my family."

Masaraure said he sought extensive counselling from multiple service providers, though recovery remains incomplete. "I've managed to overcome certain issues through counselling, including sleep difficulties and constant unsettlement. However, I'd be lying to claim complete recovery—it's something embedded in my life that I live with through memories." He said he sustained serious injuries in both incidents, with medical reports documenting severe tissue damage and scarring. However, he is withholding these reports pending legal action against his abductors, confident that proper investigations could identify the perpetrators since police officers who received him know exactly who delivered him to the station. "I remain confident that justice will eventually be served, not only for me but for other victims of power abuse—those seized with mandates to protect people but who become their enemies and threats."

Wehn human rights activist Tatenda Mombeyarara was abducted from his Chitungwiza home on 13 August 2018, he never expected to survive or see his family again. He was kidnapped by six heavily armed men who assaulted and severely tortured him before dumping him at a quarry mine near Hatfield in Harare. According to the Zimbabwe Lawyers for Human Rights, captors demanded details about an anti-government protest organised by the opposition MDC party scheduled for 16 August 2019. During interrogation, the unidentified men questioned Mombeyarara about expected attendance numbers and details about how the protest had been organised.

Narrating his ordeal to this author, Mombeyarara said his abductors were brutal. "I was stripped naked and beaten with several weapons while being interrogated about my activist work and a workshop I'd attended in the Maldives," Mombeyarara recounts. While this all happened in a short time, it felt like

an eternity considering the brutality involved. I was taken around midnight and was in the hospital around five in the morning.” Doctors who attended him at the Avenues Clinic told him that his kidneys had been badly damaged. He required atrioventricular treatment. He sustained broken bones in his left leg and ankle area, plus a finger on his left hand that required surgical screws for repair. A large, dark scar marks where a sharp object ran from his foot up his ankle. Six years have passed since his ordeal. “Rather than being silenced, this unfortunate incident has strengthened my long-held conviction that a healthy society is one where citizens have a say in how they live their lives and that the cause of justice is sacrosanct,” he says.

“I have established the Survivors of Abductions and Torture Solidarity Trust, which aims to provide survivors with group-led therapy towards healing and repurposing after the trauma, offering support for families of victims and survivors, and seek legal recourse.” Mombeyarara says he has been inspired by the desire to create a safe space for other victims of abduction and torture. “It is now six years after the

horrendous ordeal but I still struggle with panic attacks and other psychological and emotional challenges. Whenever similar incidents happen in Zimbabwe, I get triggered and become very anxious about my safety. “Without any consequences for the perpetrators and without any assurances of safety, it is difficult for survivors to feel safe. Some of the injuries are a constant reminder of the horror. The first two years, I heavily relied on clinical therapy, including anti-psychotics and sedatives. I also receive key counselling. In this regard, I thank the organizations and individuals offering critical support services to human rights defenders. As of now, I have sought and benefited from spiritual healing, meditation, and maximising on social relationships.”

However, his organisation faces bureaucratic obstacles to legal operation. “We are battling to get registered so we can operate legally. I have also written about the ordeal to encourage survivors and to offer views of survivors for purposes of policy implementation and strengthening support services. I do this because only we can free ourselves,” he says.

JOURNALISM UNDER ATTACK

Under President Mnangagwa, journalists in Zimbabwe are increasingly operating in a hostile environment characterised by intimidation and arrests, despite constitutional guarantees of media freedom and access to information.¹¹⁷

The Mnangagwa administration has undertaken several legislative reforms to align media laws with the Constitution of Zimbabwe’s Amendment (No. 20) Act, 2013. The notorious Access to Information and Protection of Privacy Act (AIPPA) was struck from the statute books in July 2020 and

replaced by three new laws: the Zimbabwe Media Commission (ZMC) Act of 2020, the Cyber and Data Protection Act of 2021, and the Freedom of Information Act of 2021.

However, these ostensibly progressive laws contain restrictive clauses that undermine

¹¹⁷ Section 61(1) provides that everyone has the right to freedom of expression, which includes freedom to seek, receive and communicate ideas and other information, freedom of artistic expression and scientific research and creativity and academic freedom. Section 61(2) stipulates that every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists’ sources of information. Veritas, “Constitution of Zimbabwe Consolidated as at 2018,” Veritas, 2018, <https://www.veritaszim.net/node/4750>.

their seemingly positive intent. More critically, the state continues deploying draconian legislation to silence journalists through intimidation and arrests. The operating environment has been further compromised by security personnel infiltrating media spaces, making independent journalism increasingly difficult. The security agencies routinely second personnel to media houses and deploy agents to monitor journalists at media and state events.

In any interview with this author, Zimbabwe Union of Journalists secretary general, Perfect Hlongwane, decried state-sanctioned surveillance and punitive media laws, abductions, torture, arrests, and enforced disappearances, which have created a deeply chilling effect on journalism in Zimbabwe. “These tactics demonstrate a systematic assault on press freedom designed to instil fear among media practitioners,” Hlongwane said. “The biggest challenge is that our laws contradict each other. Freedoms granted by one law are withdrawn by another. Progressive laws providing journalists with rights to free expression are nullified through provisions in other statutes.” Hlongwane said it was unfortunate that Zimbabwean journalists are targeted and arrested for doing their work. He said this “should not find any place in a progressive democratic society”.

This heavy-handed approach creates a shrinking operating environment that leads to self-censorship, reduced investigative reporting, and eroded public trust in media. By targeting journalists, the state undermines the media’s essential watchdog role. “While we recognise incremental gains from reform efforts, changes have been largely cosmetic since statutes still permit significant state control and surveillance. Without meaningful legal and institutional protections for journalists, this destructive cycle will continue,” Hlongwane said.

The weaponisation of enforced disappearances against journalists represents the most extreme form of state intimidation. Some of the prominent cases happened under President Mugabe’s watch but even then, Mnangagwa would have known and did not speak out against such injustices. After all, he is the self-styled Godfather of the CIO and by his own admission, nothing happens in Zimbabwe without his knowledge. In March 2015, journalist and pro-democracy activist Itai Dzamara was abducted from a barbershop in Harare’s Glenview suburb after enduring prolonged surveillance. He remains missing. There has never been an acknowledgement or attempt by the Mugabe and Mnangagwa regimes to investigate his disappearance and ensure justice is served. His case serves as a stark warning to other journalists.¹¹⁸

On 3 December 2008, journalist-turned-human rights activist, Jestina Mukoko was abducted by 15 armed men who were driving unmarked vehicles.¹¹⁹ Mukoko had widely reported on public violence that followed the defeat of President Mugabe by Morgan Tsvangirai in the 2008 presidential elections. Mukoko was the director of the Zimbabwe Peace Project, a civic society organisation. During her two-week detention, Mukoko endured torture, including simulated drowning, confinement in a freezer, and physical assault as her captors attempted to force confessions to charges of recruiting people for military training to overthrow the government. The Supreme Court granted a permanent stay of prosecution in September 2009 due to fundamental rights violations by state security. In 2018, the High Court ordered state compensation for unlawful prosecution and suffering at the hands of security agents. Mukoko’s ordeal exemplifies how surveillance-enabled persecution creates lasting trauma that extends beyond individual victims. Her case has had a

118 Amnesty International, “Zimbabwe: Ten years without answers since journalist and activist Itai Dzamara’s enforced disappearance.” Amnesty International, March 7, 2025 <https://www.amnesty.org.zw/2025/03/zimbabwe-ten-years-without-answers-since-journalist-and-activist-itai-dzamaras-enforced-disappearance/>.

119 Frontline Defenders, “Jestina Mukoko Abducted,” Frontline Defenders, 2008, <https://www.frontlinedefenders.org/en/case/jestina-mukoko-abducted>.

particularly chilling effect on young journalists entering the profession and discourages female journalists from political coverage, demonstrating how targeted persecution strategically narrows the scope of democratic discourse.

Recent cases under President Mnangagwa's watch reveal how surveillance technologies enable targeted harassment of journalists through strategic arrests. Blessed Mhlanga of Alpha Media Holdings (AMH) spent 72 days in pretrial detention after being charged with inciting violence under Section 164 of the Criminal Law (Codification and Reform) Act. His employer, Heart & Soul TV, an AMH subsidiary, faces similar charges for broadcasting a press conference where war veteran Blessed Geza called for President Mnangagwa's resignation.¹²⁰ Mhlanga has since filed a Constitutional Court application challenging his arrest.

Mhlanga told this author that there was nothing criminal about the charges he is facing, describing them as "political charges". This marked his eighth arrest, though his longest detention period. "I was once arrested for allegedly practising journalism without a press card, even though I had already applied for it and carried the card in my wallet. They seized my belongings, found the card, but still detained me for two nights," Mhlanga recounted. "They have always been after me. They target my work specifically. If I stayed home, they wouldn't arrest me."

Mhlanga said it is ironic that President Mnangagwa's regime is now persecuting him when he gave him a platform to speak out when he (Mnangagwa) was being persecuted by President Robert Mugabe in 2017. He said he risked so much to give Mnangagwa an opportunity to be heard when other journalists feared covering his story. "I was the one who was doing his story. I had

meetings with Mnangagwa at his house in Belvedere (Harare). He dictated his last press statement during the (2017) coup (which ousted Mugabe), while I typed on my computer. I printed it and he acknowledged and signed it. "He asked me to give the statement to other journalists because he could not do it himself. He was afraid of being arrested. I shared the documents with fellow journalists. I gave them a voice when they wanted a voice. But now that I'm giving someone else a voice and it hurts him (Mnangagwa)," Mhlanga said.

Prominent journalist Hopewell Chin'ono was arrested three times between 2020 and 2021. In 2020, he was charged with 'incitement to commit public violence. This was after he re-tweeted a post by opposition politician, Jacob Ngarivhume, who was calling for a national shutdown in protest of poor governance by President Emmerson Mnangagwa's administration. As with other cases involving journalists, Chin'ono was tracked to his home. He live-streamed his arrest on social media, with the police breaking into his house, and was only released on bail on 2 September 2020. That same year, he was arrested after he tweeted that he had spoken to some members of the National Prosecuting Authority (NPA) who told him that Henrietta Rushwaya, a controversial gold dealer, would be granted bail in a case where she had been arrested on gold smuggling charges. The state accused him of having links to the NPA.

In 2021, Chin'ono was again charged with publishing falsehoods under Section 31 of the Criminal Law (Codification and Reform) Act which deals with "publishing or communicating false statements prejudicial to the State."¹²¹ The state pressed the charges despite the Constitutional Court outlawing this statute in 2014 following a challenge by Zimbabwe Independent journalists. This

120 Amnesty International, "Zimbabwe: The arbitrary detention of journalist a brazen attack on press freedom," Amnesty International, February 2024, 2025, <https://www.amnesty.org.zw/2025/02/zimbabwe-the-arbitrary-detention-of-journalist-a-brazen-attack-on-press-freedom/>.

121 Mary Taruvinga, "LATEST: Journalist Chin'ono arrested again." New Zimbabwe, January 8, 2021. <https://www.newzimbabwe.com/latest-journalist-chinono-arrested-again/>

selective application of invalidated laws reveals the state's willingness to weaponize legal uncertainty against media practitioners.

ESCALATING DIGITAL SURVEILLANCE AND INTIMIDATION

Recent developments indicate that the Mnangagwa administration is not slowing down in its assault on journalists. If anything, the regime is expanding surveillance capabilities that extend beyond physical monitoring to comprehensive digital oversight. In February 2024, investigative publication NewsHawks was forced to abandon follow-up stories on military corruption after receiving direct threats from state security agents. News editor Owen Gagare was placed under surveillance, creating a chilling effect that demonstrates how targeted monitoring can effectively silence entire investigations.¹²² The sophistication of surveillance operations had already been evidenced by a 21 December 2022 incident wherein investigative journalist Mary Taruvinga was threatened into abandoning an investigation she had not yet begun working on. The state's advance knowledge suggests comprehensive monitoring of journalists' communications and planning.

Online intimidation has become increasingly brazen. On 20 April 2024, Presidential spokesperson George Charamba used his

X platform to threaten journalists. "Very soon, we will reach a stage where carrying or repeating stupid, disruptive messages will attract lawful punishment. You cannot circulate alarm and despondency and go scot-free!!!! Before long!!!!" Charamba's threat specifically targeted journalists covering Blessed Geza's calls for President Mnangagwa's resignation.

Media Institute of Southern Africa (MISA) Advocacy and Communication Chairperson Mlondoloz Ndlovu identifies problematic and bad laws as the foundation enabling systematic persecution. "The Interception of Communications Act allows the state to monitor people's devices with very limited restrictions," he explained. "This is a law that was passed before the current Constitution, which explicitly provides for rights for the freedom of expression and the freedom of the media. He said while AIPPA's repeal appeared progressive, criminalisation of journalism persists through the Cyber and Data Protection Act as well as the Criminal Law Codification and Reform Act.

"Journalists fear performing their duties because they understand the state's potential response. For example, Blessed Mhlanga and others were arrested without any evidence of any crimes. They were arrested just to intimidate them. What happened to Mhlanga has a chilling effect on journalists. So the fear of arrest leaves others fearful of surveillance which is done physically and digitally," Ndlovu said.

¹²² Media Institute of Southern Africa (MISA), "NewsHawks freezes military story," Media Institute of Southern Africa, 2024, https://misa.org/blog/media_violations/newshawks-freezes-military-story/.

CONCLUSION

Zimbabwe's evolution into a sophisticated, technologically enabled surveillance state under successive ZANU-PF administrations reflects a deeply entrenched trajectory of authoritarian consolidation, rather than the long hoped-for break from legacies of its colonial past.

Despite constitutional guarantees, democratic institutions have been systematically eroded by a multi-layered surveillance architecture—encompassing physical, digital, legal, and informal mechanisms—with deleterious effects on human rights, civic life, and democratic practice.

The current era under President Mnangagwa reflects more than just an incremental intensification but more significantly a qualitative transformation: algorithmic and preemptive surveillance now enables regime security at the expense of genuine national security, rendering dissent dangerous both on and offline. The fusion of domestic repression mechanisms with sophisticated external technologies—often procured in secrecy and without any oversight—concretizes the vulnerability of citizens and particularly targets opposition activists, journalists, and human rights defenders with impunity.

The Zimbabwean experience should not be seen as an inevitable and irreversible; it should be seen as a signpost on the dangers of unchecked surveillance and its facilitation of authoritarian entrenchment. The documented resilience of journalists, civil society, and survivor advocacy groups offers persistent hope and a basis for reform. International actors, local stakeholders, and Zimbabwe's own citizens must remain resolute and continue the fight to reclaim democratic space by demanding transparency, accountability, and the restoration of constitutional rights and freedoms.

RECOMMENDATIONS

Persons at high risk of state surveillance should ensure they are digitally secure, given that state security agents are increasingly

monitoring citizens online. These include journalists, human rights defenders, politicians, political activists, and trade unionists. This can be done through regular trainings to capacitate them to identify and mitigate cybersurveillance risks. Persons at risk should in turn ensure that people in their circle are cyber secure, so that they are not compromised through them. Please check Intelwatch's security manuals for reporters and human rights defenders. Below are a few pointers from these manuals.

Digital security measures to be taken include:

- The use of encrypted communication and using end-to-end encrypted messaging applications like Signal
- The use of Virtual Private Networks to mask IP addresses
- Ensuring they never leave gadgets like cell phones and laptops unattended while also logging out of their emails
- Use Password Manager to keep passwords for their various accounts, use strong passwords and enable two-factor authentication.
- Storing Sensitive Data using encrypted external drives or cloud storage with a strong password
- Securing devices by regularly updating software,
- Utilising tools like Tor for anonymous browsing
- Being cautious of phishing attempts and malware
- Physical security is also important given the ever-present threat of abductions and physical harm.
- Physical security measures that can be taken include:
- Ensuring adequate home security where

possible, including CCTV, biometric security, alarm, dogs and ensuring the yard is well lit

- Ensuring secure locations for meetings and activities. Create check-in practices to ensure someone always knows where you are.
- Being aware of surroundings, signals or behaviours indicating surveillance (e.g., unfamiliar people, strange vehicles)
- Avoiding predictable behaviour and travel patterns
- Conducting meetings in public places, especially with people one is not too familiar with.
- Advocacy and Support is essential for those at risk. This includes:
- Campaigning for the repeal of retrogressive laws through advocacy and pressure. Regional and international pressure groups and professional bodies, such as journalism groups or trade unions, can also be roped in for support and solidarity
- Lobbying multilateral institutions such as SADC, the African Union, United Nations and the European Union, among

others could help build pressure on the Zimbabwean government to institute the necessary legal, security sector and institutional reforms to ensure the respect for civil rights and democratic governance

- Having access to human rights lawyers as well as regional and international human rights bodies for support and help when legal assistance is needed
- Networking with professional bodies that can offer assistance when in trouble. Journalists for example, can link with Reporters Without Borders or the Committee to Protect Journalists
- Building a local network for peer support, mutual protection, information sharing, whistleblowing, best practice sharing and security awareness

It is vital for journalists, human rights defenders, political activists and other vulnerable persons to seek regular training on subjects such as digital and physical security, first aid and legal matters.