The militarization of digital surveillance in post-coup Zimbabwe: ‘Just don’t tell them what we do’

Allen Munoriyarwa
University of Johannesburg, South Africa

Abstract
While a large body of research has documented and theorized digital surveillance practices in various political contexts, little has been done to investigate the growing trend of military-driven digital surveillance practices in semi-authoritarian regimes. In this article, I use the case of the surveillance practices of the Zimbabwe Defence Forces to argue that scholarship needs to (re)evaluate this emerging trend. The article has three aims: first, it explores military-driven surveillance capabilities, the circulation of such capabilities and the surveillance tactics emerging in the semi-authoritarian context of Zimbabwe. Second, it examines the interface of factionalism and politics within the Zimbabwe Defence Forces and how this influences quotidian military-driven digital surveillance practices. Third, it locates military-driven surveillance practices within a growing and complex global political economy of trade in surveillance technologies that is centred on China. In doing so, the article helps locate a largely neglected but increasing practice of military-driven surveillance that is incrementally reconfiguring surveillance practices and architectures in semi-authoritarian regimes. Such a form of surveillance provides gateways for human rights abuses and shrinks the civilian spaces of protest and engagement, leading to digital authoritarianism. The article therefore calls for greater scrutiny of the emerging practice of military-driven digital surveillance in semi-authoritarian political contexts.

Keywords
Assemblage, capabilities, digital surveillance, Zimbabwe Defence Forces

Introduction
Military-driven surveillance in Zimbabwe is a dynamic and rhizomatic assemblage of technologically mechanized practices embedded within different units of the Zimbabwe Defence Forces (ZDF) and utilized in various contexts. It is a consequence of two converging factors. One is the growing role of start-up Chinese companies as suppliers of affordable surveillance technology; the other is a hardening military-driven political authoritarianism in post-coup Zimbabwe. In this article, I explore the various manifestations and mutations of military-driven digital surveillance in post-coup Zimbabwe. The ZDF has incrementally amassed digital surveillance capabilities that allow it to engage in extrajudicial digital surveillance using various tactics. Furthermore, the ZDF’s
surveillance capabilities and the circulation of its surveillance practices are largely tempered by politics and factionalism within the institution itself. In order to understand the capabilities, circulation and tactics of surveillance within the ZDF, we need to relate this to China and its start-up technology companies as enablers of military-driven surveillance practice.

The observations made above allow me to sustain three inter-related arguments. First, I argue that a close study of Zimbabwe confirms that the interests of political actors are materializing in digital surveillance practices in ways that are leading to a militarization of civilian spaces and a civilianization of military surveillance. This leads to my second argument, which is that the dispersal of military surveillance technologies, filtering rhizomatically into civilian spaces, is morphing into an elaborate oppressive and weaponized network of military-driven political repression. The third argument I make is that the involvement of China and Chinese-based technology companies in the ZDF’s surveillance practices has reconfigured the ZDF’s surveillance architecture. Chinese involvement in Zimbabwe’s military-driven surveillance practices syncs with Beijing’s pursuit of its broader geopolitical objective of increasing Chinese influence in Africa and, in the process, outmanoeuvring the West. Therefore, semi-authoritarian regimes like Zimbabwe have become a crucial vector for the expansion of digital surveillance and the development of an international market of surveillance technologies.

In the article, I draw on Haggerty and Ericson’s (2000) concept of the surveillant assemblage in two ways. First, I explore their assertion that an assemblage of surveillance capabilities now links the surveillance capacity of multiple and rhizomatic systems (and players) throughout society. This has potentially captured everyone in its decentralized and distributed web, with groups that should be exempted from surveillance increasingly being targeted (Haggerty and Ericson, 2000). In the specific case of Zimbabwe, we see how the military has developed a decentralized surveillance system that targets civil society and legitimate political opponents of the ruling party to which the ZDF is aligned. Second, the notion of the surveillant assemblage is helpful for efforts to understand military-driven surveillance in Zimbabwe as a result of the claim that the surveillant assemblage has given rise to new configurations of surveillance (Haggerty and Ericson, 2000). Military-driven surveillance itself should be understood as part of this new configuration taking root in semi-authoritarian contexts.

The concept of the surveillant assemblage thus explains how, in military-controlled political contexts, surveillance forms part of a decentralized practice that is currently increasing in both capacity and efficiency. I move beyond the current conceptualization in two ways. First, I use the Zimbabwean case to show how the rhizomatic or discrete assemblages wrought by multiple connections across a myriad of technologies and practices go beyond ‘the desires for control, governance, security, profit and entertainment’ (Haggerty and Ericson, 2000: 609). I demonstrate that, in military-driven semi-authoritarian contexts, the assemblage is occasionally weaponized in efforts to create a politically oppressive surveillance system that surveils legitimate political opposition. Second, the rhizomatic assemblage is tied to regimes of power (in this case, the military). The assemblage is accordingly a culmination of multiplicity: it is not simply an attribute, a single assumed unity, but rather consists of multiple units and assumes multiple manifestations. In addition, this article notes that while the concept of the assemblage accounts for the decentralized, rhizomatic and emerging surveillance configurations in Zimbabwe, it is not adequate for explaining the external role of China in the development of surveillance networks in Zimbabwe. The macro-level circulation of surveillance tools – or what I call the ‘Beijingification’ of the global trade in surveillance tools – cannot be understood through the lens of the surveillant assemblage.

The article adopts an exploratory approach because, in the emerging discipline of surveillance studies, the domain of military-driven surveillance practices, especially in semi-authoritarian political contexts like Zimbabwe, has been markedly neglected. In this article, I make several
intellectual contributions to existing scholarship. At a broader level, I seek to contribute to nascent debates on digital surveillance in the Global South – Zimbabwe in particular. I also contribute to an understanding of digital surveillance in semi-authoritarian regimes. The field of military-driven digital surveillance has received scant academic attention in surveillance research. Furthermore, surveillance research in Zimbabwe itself remains patchy, despite the country’s well-documented militarization of state institutions. Lastly, the increasing role of China and Chinese technology companies in driving the growth of digital surveillance in Africa remains underresearched. By making this contribution, I situate the less-explored phenomenon of military-driven surveillance studies within critical security studies that explore the ways through which semi-authoritarian regimes appropriate digital surveillance technologies for political purposes and in ways that endanger the security of individuals.

I will first sketch the political context of Zimbabwe by providing a brief synopsis of the country’s semi-authoritarian regime. This is important for our understanding of the growth of military-driven digital surveillance in the country.

The context: Zimbabwe’s semi-authoritarian political regime

Since its independence in 1980, Zimbabwe has been governed by a semi-authoritarian regime. Semi-authoritarian regimes occupy the grey area between fully fledged authoritarian regimes and democracies (Ottaway, 2003). They embody, broadly, three major characteristics: first, they manipulate elections (Levitsky and Way, 2003); second, they create the façade of democratic institutions but weaken them (Ottaway, 2003); and, third, the latter institutions often operate in the interests of the ruling elites (Levitsky and Way, 2003). State institutions such as the military fall under the regimes’ ‘menu of manipulation’ (Schedler, 2002). Zimbabwe fits all three parts of this description because there is a rhetorical acceptance of liberal democracy and formal democratic institutions, yet they exist in attenuated forms. For example, former president Robert Mugabe unleashed violence in 2008 after losing a presidential election. He mobilized the ZDF, the Zimbabwe Republic Police (ZRP) and secret services organs clustered in the Central Intelligence Organization (CIO) to launch a scorched-earth election campaign on his behalf. Paradoxically, on 17 November 2017, Mugabe was toppled from power by the security organs of the state that had consistently backed him since 1980, in favour of his then vice-president, Emmerson Mnangagwa.

The conflation of the state and ruling-party politics has been a characteristic of postcolonial Zimbabwe. Members of the military have been appointed to lucrative state and parastatal board and executive posts. Prosecutors from the ZDF have been seconded to civilian courts. Active military personnel serve in government ministries. Currently, the country’s cabinet is dominated by former military personnel, and the parliamentary caucus of the ruling party, the Zimbabwe African National Union-Patriotic Front (ZANU-PF), is dominated by former soldiers. This underlines the symbiotic relationship between the military and the ruling party. Tendi (2020) notes that, in the post-coup era, Zimbabwe’s military has gradually encroached on civilian spaces. For example, members of the ZDF have been involved in the arrest of opposition party politicians, despite the fact that, under the 2013 constitution, they do not have powers of arrest. Ruhanya (2018) argues that this newfound role of the ZDF has come with its involvement in keeping ZANU-PF in power.

In recent times, the military has been exposed as having been involved in the surveillance of leaders of opposition parties, civil society organizations (CSOs) and anti-regime churches, as well as independent journalists and other anti-regime activists. These exposures have led to lingering questions: how extensive is the use of such practices by the military? What are the ZDF’s interests in surveillance? Who are the enablers and who are the major targets of this practice? These practices should be understood as a response to economic, political and social developments in Zimbabwe.
In the face of a deteriorating economy, rising unemployment, corruption and general disillusionment, opposition to the ruling party has intensified. Protests have flared up in the country’s restive urban areas. The military has tightened its grip on politics to prop up ZANU-PF’s waning political dominance (Ruhanya, 2018). As part of this, the military now involves itself in civilian digital surveillance, an area constitutionally fenced off from its reach (Media Policy and Democracy Project (MPDP), 2019). The presence of a partisan judiciary (Magaisa, 2019) has dented all hopes of judicial intervention in the service of human rights. Before delving into the military’s involvement in surveillance practices in Zimbabwe, it is important to flesh out the emerging literature on digital surveillance in semi-authoritarian regimes in general, along with the small but crucial literature on military-driven surveillance of civilian spaces.

**Military-driven surveillance and semi-authoritarian regimes**

For more than a century, surveillance has been understood as a military practice associated with the provision of security (Jensen, 1991: iv). There is an accepted view that modern-day technology-based surveillance practices have their genesis in the military (Wilson, 2012). In colonial times, the military was involved in surveillance against espionage, treason and revolutionary activities (Jensen, 1991: 12). Ogasawara (2019: 726) notes that military-driven surveillance in colonial times was often severe and violent. But, as Berda (2013: 627) argues, colonial military surveillance practices were often violent because they were meant to ‘manage dangerous populations’ of people who were opposed to colonial practices of violence and extraction. Violence and extraction formed the backbone of the survival of the colonial system itself. Berda (2013) notes that we should therefore understand contemporary military-driven practices as offshoots of colonial military practices. What is discernible in this literature is that colonial military-driven surveillance targeted the racially different other, the rebel who opposed the violent extraction of the colonial system.

The Zimbabwean case demonstrates a new form of postcolonial military-driven surveillance that is no longer targeted on the racially different other, but is instead carried out by the military to safeguard and protect a ruling party from legitimate political opposition, and thus represents a weaponization of the practice against the party’s legitimate opposition. Such a practice is prevalent in many semi-authoritarian contexts, such as Turkey (Yonucu, 2018) and Morocco (Hagmann, 2021). In Turkey, for example, Yonucu notes that surveillance is used to wage war against oppositional politics and to reconfigure the local political space. Hagmann (2021) agrees with Yonucu, noting that in Morocco urban spaces are often secured by tech state surveillance, which leads to controlled urban spaces without freedom. Surveillance in the Global South is a manifestation of contemporary controlled societies (Hagmann, 2021; Yonucu, 2018). Yonucu (2018) argues that contemporary societies experience various forms of urban policing, with surveillance included among the strategies for such policing.

Other researchers have argued, however, that the militarization of digital surveillance is not a new phenomenon (Howell, 2018; McMichael, 2017). Surveillance has often been a militarized practice. Howell (2018: 117) argues that we cannot ‘falsely presume a peaceful liberal order that is encroached on by military values or institutions’. Howell’s argument is that both civilian and military life are imbricated through martial policies and war-like relations. Neocleous (2015) agrees with Howell, further stating that in the neoliberal global security order civilian life and the everyday practices of state security apparatus are often conflated. Thus, security agencies often make use of civilian institutions, and vice versa, while traditional lines between war and policing are blurred (Neocleous, 2015). McMichael (2017: 115) makes a similar assertion, noting that ‘war and police power do overlap and conjoin in everyday pacification’. According to Seigel (2018), it is therefore fallacious to assume that civilian policing is distinguishable from the military. Since policing is the
human-scale expression of the state, it is inevitably militarized, since the military is the quintessential translation of state power.

Nevertheless, the Zimbabwean case represents a new kind of military urbanism – one that is aimed at anti-regime activists and political opponents. Zimbabwe accordingly exhibits a phenomenon that stands out as politically motivated military-driven surveillance urbanism. The military enjoys an advantage in surveillance. It is an entity that has the experience required for the organization of large-scale and complex surveillance enterprises (Dandeker, 2006) with the relative secrecy such enterprises demand. The Zimbabwean case is complicated by other factors. These include pervasive violation of human rights by the military itself. In democratic political contexts, civil movements have expanded to constrain militaries from involvement in internal surveillance practices. Postcolonial Zimbabwe, however, has not produced institutions capable of constraining military encroachment into civilian private spaces. Nagy (2017: 453) makes similar observations about post-transitional Hungary, establishing that ‘extended surveillance practices . . . are used as an instrument of a political deterrence strategy against political opponents’. Wilson (2012: 270) adds that military surveillance is part of the concoction of power in semi-authoritarian regimes. In Myanmar, for instance, the military is central to surveillance practices, which are enabled by its huge size and large budget. Wilson (2012: 270) specifically argues that ‘[military] surveillance for political and social control continues, while the spread of mobile communication devices . . . has opened up more extensive . . . opportunities for monitoring’.

There are three key conclusions that I draw from this literature. First, in most countries, the military enjoys a greater ability to surveil than any other security institution. Second, in semi-authoritarian regimes, oppressive and opaque forms of surveillance practices are becoming increasingly ubiquitous. Lastly, in some contexts in which the military takes on an arbiter role within politics, military-driven surveillance is a common practice. There are gaps in the literature that still need addressing, however. For instance, beyond the case of Myanmar (Wilson, 2012), research on how and why the military drives civilian surveillance remains lacking. In this article, I tread at the interface of these studies and thus contribute to an emerging area of scholarship – namely, the study of military-driven digital surveillance. In the next section, I briefly outline my methods.

**Methodological issues**

This article draws on nine key in-depth respondent interviews with recently retired military personnel who had migrated from Zimbabwe and former members of ZANU-PF, exiled post-coup, who have inner working knowledge of the country’s military surveillance architecture. The article complements these interviews with documentary analysis – relying on mainstream news reports on surveillance practices and reports of civil society organizations about digital surveillance in the country. By its very nature, this research is sensitive, which explains the limited number of informants. Military personnel always run the risk of being persecuted for discussing military issues, especially in countries like Zimbabwe, where the army has gained notoriety for brutalizing citizens (Masunungure, 2011). However, I should point out that in a research project as sensitive as the present one, interview data may present their own limitations. One such limitation is that informants may be prone to ‘snap judgements’ of the situation under investigation since they are not exposed to the whole surveillance picture within the ZDF, but only that of the particular department in which they are domiciled. In addition, cross-verification of informants’ information is difficult where informants prefer anonymity.

The research followed elements of the framework developed by Dempsey et al. (2016) for the conduct of sensitive research. Such a framework includes in-person and face-to-face meetings with respondents to build closeness, along with meeting respondents at a time and location of their
convenience to build trust. In line with this, this research was conducted in places across southern Africa. Additional measures for the conduct of sensitive research outlined by Enosh and Buchbinder (2005) were also adopted. These involved ensuring anonymity and confidentiality for respondents.

Findings

In the first subsection of the findings, I examine the circulation, capabilities and tactics of the ZDF’s surveillance culture. This will allow me to explore, in the second subsection, how politics and factionalism within the ZDF affect everyday surveillance practices. The presentation of these two issues will then enable me to explore the global political economy of surveillance technology acquisition itself, where I highlight the role of China as a major enabler and its implications. I conclude with a discussion that puts the consequences of military-driven surveillance practices into a broad context.

Capabilities, circulation and tactics

The ZDF’s surveillance capabilities are domiciled in numerous ZDF units, especially Military Intelligence (MI), the Special Air Service (SAS) and the Signals Unit (SU), which have been accumulating a vast array of surveillance equipment that allow them to undertake public space and communication surveillance (MPDP, 2019). The capabilities, moreover, lie primarily in two domains. These are public-space surveillance capabilities and cyber-communication surveillance capabilities.

The ZDF’s digital surveillance capabilities have become increasingly sophisticated, boosted by several internal factors. First, relatively huge budget outlays provide the ZDF with a sound financial footing that enables it to actively purchase surveillance equipment. Indeed, the ZDF has enjoyed a huge portion of the total national spending from the fiscus for many years in a row, from about the year 2000 (ZIMCODD, 2020). This gives the institution ‘an ability to leverage these funds towards critical purchases of the technology that we want. When the money is available, it is even easy to negotiate for continuous purchases. We also have additional advantage of . . . getting more guarantees from the national fiscus’ (Interview 1). In addition, availability of funding is crucial to the accumulation of a growing array of digital surveillance technology, along with the essential steps that follow acquisition, such as ‘having to send the people to our suppliers for training on how to use these complex technologies . . . a step we cannot choose to ignore’ (Interview 2).

In addition to funding, what I call ‘political activity indicators’ are an important factor driving the ZDF’s growing surveillance capabilities and practices. The political activity indicator ‘is about which group ought to be placed under surveillance at any particular time. . . . Not all opposition groups present the same level of threat. . . . Our targets do mutate, but the objective remains the same. . . . Political threats to the system [are] the main consideration, and it determines the tactics as well’ (Interview 3). One prominent practice employed is ‘the spread of surveillance capabilities’, which is necessitated by the desire to ‘maintain blanket cover of the practice, especially from civil society organizations’ (Interview 3). According to informants, the spreading of capabilities means that different units within the ZDF are trained and equipped for specific surveillance practices. As one respondent noted, ‘At the Robert Mugabe College of Defence, you will find bulk data interception technologies. At the Special Air Services units, you will find cellphone tracking units domiciled there, and other forms of electronic communication surveillance. . . . And at the military police units, you will find biometrics and geolocation technologies’ (Interview 4). When certain units specialize in specific forms of surveillance, jurisdictional issues are solved, as each unit
assumes responsibility for a specific form of surveillance. This leads to specialization, which enhances skills, and a further reinforcement of surveillance capabilities.

Military-driven surveillance practices form a fluid system. The enemies of the ruling regime are not cast in stone; as opposition mutates from political parties to social movements and CSOs, the ‘menu of surveillance’ that the military undertakes also varies. This confirms a less disputed fact, namely, that the ZDF’s surveillance practices have nothing to do with fighting terrorism or augmenting police and intelligence agencies’ efforts against crime (MPDP, 2019). Semi-authoritarianism thrives on manipulating state institutions (Schedler, 2002). In this case, the ZDF becomes part of ZANU-PF’s political survival and power matrix. The military-driven practices tap into the ‘political mood’ and prepare the ruling regime for counter-action against even legitimate opposition. In the ‘menu of surveillance’ available to military personnel in different units, the severity of surveillance, according to one respondent, is equally determined by ‘the technologies that each unit has at its disposal. . . . Some are well-equipped for cyber-communication surveillance, others have technology for public space surveillance. . . . It does not mean these units because they belong to one entity have the same capabilities’ (Interview 5). It is difficult to cross-reference data from state actors. This is because of the nature of the subject under discussion, as well as the fact that some respondents may be acting out of their own frustrations. Overall, however, this does not render their testimonies doubtful.

We should therefore imagine the ZDF’s surveillance practices as a series of assemblages distributed across different units of the ZDF. But actors in these assemblages do not act as one fluid and cohesive unit. They are disparate actors spread across several meta-units of a monolithic institution in rhizomatic fashion, with no known meaningful coordination. The senior command makes the final decision, in liaison with the ruling political elites. Such dispersal of practices is a double-edged sword for the ZDF. On the one hand, dispersing surveillance practices across several units makes it difficult for would-be activists to pinpoint responsibility and apportion it to a single entity. It also gives the advantage that the ZDF is assured of numerous flows of data from these different units, an advantage that would be diminished if surveillance practices were institutionalized in one unit of the ZDF. The disadvantage is that when surveillance becomes rhizomatic, as in this case, it becomes difficult to coordinate, and the possibility of data leakages increases. This possibility can easily be seized upon by activists.

These observations bring me to the following question: what kind of capabilities does the ZDF possess? Surveillance technology within the ZDF includes an assorted assemblage of facial recognition devices from CloudWalk, a Chinese technology company (Global Times, 2018); CCTV cameras from HikVision, another Chinese company (Standard, 2020a); and international mobile subscriber identity catchers (‘IMSI catchers’) from Iran that have, according to sources, been used recently to track political opponents. It should be emphasized that this demonstrated surveillance power on the part of the military raises serious legal concerns for the anti-surveillance activists, human rights advocates and opposition party members who are its targets. One of these concerns is that, under Zimbabwe’s 2013 constitution, the country’s military can only be involved in ‘external surveillance’ – that is, surveillance of external threats. I argue that the demonstrable growth of the military’s surveillance capabilities constitutes a unidirectional flow of surveillance capacity that is evidently shifting away from civilian institutions such as the Central Intelligence Organization (CIO) and the Police Internal Investigations Services (PISI), the state institutions constitutionally tasked with practising surveillance related to crime fighting. Indeed, Zimbabwe’s CIO was caught in the succession fight that pitted former president Robert Mugabe against the current president, Emmerson Mnangagwa. Noyes (2018) notes that, in the post-coup era, seasoned CIO officers were forced out or transferred to non-intelligence institutions. For example, a well-known CIO boss died under torture at a military barracks during the coup. The surviving
spouse sued the military in the High Court (Taruvinga, 2019). This was not an isolated incident, but part of the regime’s modus operandi even before the coup. Noyes (2018) has described the ascendancy of the military in intelligence gathering as a swift reward for its role in enabling Mnangagwa’s rise to power. Noyes further notes that, in the post-coup period, the CIO has been underfunded and has been unable to produce meaningful intelligence, leaving the military to enjoy a unidirectional production of surveillance intelligence. This attenuation of the civilian institution constitutionally mandated with responsibility for surveillance raises a number of issues. This attenuation signifies a dangerous drive towards normalizing military surveillance in civilian spaces. As one respondent noted, ‘The capacity of the military to surveil on you [sic] has become larger than that of the CIO. . . . Mugabe started this practice . . . but what I remember is that the military has become more equipped for surveillance . . . and the capacity is being exploited fully by the authorities. . . . Those of us who are close know that this is happening, and we also know the targets’ (Interview 6). It also indicates how different the Zimbabwean case is from other contexts – for example, that of the UK, where MI5, MI6 and GCHQ coordinate with other agencies in the military (Gill, 2012), or that of the USA, where the Federal Bureau of Investigation and the Central Intelligence Agency work in tandem to share intelligence relating to terrorism and other national security threats (Greenberg, 2012). The difference lies in the fact that the latter are advanced liberal democracies, while Zimbabwe is a struggling semi-authoritarian regime with a military deeply embedded in the country’s political power matrix.

I wish to highlight two major issues in relation to circulation, capabilities and tactics. The first is that circulation should be understood in two senses. The first of these relates to how the surveillance technology is owned within the ZDF. The second concerns how it is appropriated within civilian spaces. In terms of the first, I have shown that circulation is enabled by both human (i.e., the people who operate the surveillance technologies) and non-human factors (i.e., the technology itself). As one interviewee notes, ‘The human factor is as good as the availability of the technology. . . . The ZDF is careful about selecting the people with the right ideological mindset. . . . ruling-party supporters. . . . The vetting there is strict’ (Interview 5). At the core of circulation, then, are the people behind the technology, who ‘should have been born and bred . . . and conditioned within the ruling party’s political environment . . . and understand the relationship between the practice and the survival of the ruling party’ (Interview 2). Ultimately, these ‘ideologically conditioned’ operators then decide the dispensability or indispensability of certain surveillance practices in accordance with the level and intensity of opposition to the ruling party at any given moment. This brings me to the point that I can call ‘surveillance rationality’. By this I mean that military-driven digital surveillance in Zimbabwe can only be understood clearly if it is juxtaposed with the political and ideological predilections of the ZDF and its support of ZANU-PF, along with the extent to which the ZDF is willing to sustain ZANU-PF’s political survival. Makumbe (2009) has argued that to understand the ruling ZANU-PF, we need to understand that it can no longer survive the opposition onslaught without resorting to the support of the security institutions. I therefore argue for an extension of Haggerty and Ericson’s theory to include the notion of the ‘surveillance rationality’. If we are to understand the extent to which surveillance becomes rhizomatic, we should equally understand the rationales of the players. The more the players get entangled in surveillance, the more they form even deeper rhizomes that, in semi-authoritarian regimes, implicate them in extra-legal, politically motivated surveillance practices.

The second issue I want to highlight is what I might call ‘the interaction of surveillance tactics’. What I have established in this article is that various units within the ZDF do indeed practice digital surveillance. In this subsection, however, I also need to discuss the level at which this plethora of actors within the ZDF interact, in terms of sharing tactics and capabilities. As one of
my respondents said, ‘Surveillance units within the ZDF report to their various unit command-
ers, who then report along the vertical hierarchy of power’ (Interview 4). According to respond-
ents, there is no possibility of horizontal collaboration. That is only possible at the level of the
Joint Operations Command (JOC), where ‘senior commanders, who are the real, real political
beings meet with politicians’ (Interview 8). The surveillance practices that happen across multi-
ple spaces and temporalities within the ZDF find a little measure of coordination in the JOC. The
JOC does not signify an attempt by the political and the military elite to provide close coordina-
tion of the disparate activities conducted across various military units. As one respondent noted,
‘The whole public space surveillance practices we have – like specific CCTV cameras in public
spaces, border crossings – are effective at tracking down our mobile targets. On the other hand,
our cell site location information (CLSI) helps other military units track both mobile and
station[ary] targets’ (Interview 8). This leads up to the JOC. Because the information that the
JOC receives comes from separate units that often do not work in coordination, the JOC becomes
a receiver of different pieces of information. As the assemblage theory asserts, the JOC as an
institution provides a face of surveillance coordination, yet in reality there is no coordination at
all, but rather a loose gathering of different surveillance information from the different units
within the ZDF.

This shift of power towards military institutions, away from civilian spaces, is a conse-
quence of, among other factors, the fluid nature of rhizomatic surveillance (Lyon, 2006),
which allows the practice to be spread and not confined to one space, even within the same
institution. The expansion of diverse forms of surveillance means that there is no longer a need
for a single ground and institution on which surveillance can settle (Basturk, 2017). Rather,
state institutions, such as the military, can operate like flows in the process of surveillance
(Basturk, 2017), reorganizing and reappropriating state power. A 2019 report from the Media
Policy and Democracy Project corroborated the evidence provided by the previously cited
respondent, noting that the ZDF has sufficient technical capabilities to intercept communica-
tions and is boosting its personnel’s technical capacity (MDPD, 2019). In addition, the capa-
bility of the military to surveil was further confirmed by the commander of the ZDF, Brigadier
Edzayi Chimonyo, who declared that anyone working on a networked computer is under sur-
veillance (Standard, 2020b). The deputy commissioner of the police stated that the country
had received the latest surveillance equipment (Ndlela, 2020). While such a practice repres-
sents a danger to political elites that are losing public confidence and popularity, it is impor-
tant to understand the behaviour of the Zimbabwe regime when it is confronted by pro-change
movements. It always act violently to suppress such movements (Ruhanya, 2018). The increas-
ingly limitless capacity of the ZDF to surveil is also testimony to how the ZDF has been able
to drive an elaborate vertical network of surveillance operating insidiously because of its lack
of constitutionality in the Zimbabwean context (MPDP, 2019). The ZDF’s military intelli-
gence and signals units were originally purposed for military-related external surveillance
(Rupiya, 2013), but their repurposing towards civilian surveillance is testimony to the ZDF’s
growing power in civilian spaces and its desire to promote a military model of civilian surveil-
lance. The interaction of military-driven surveillance practices with an already repressive and
authoritarian political environment illegitimately restricts dissent against the ruling status quo.
It silences the views of opposition and CSOs and, in the process, hastens the country’s drive
towards the fully fledged authoritarian regime that CSOs have warned about. In addition to
this, it restricts civil liberties and shifts the goal of surveillance from crime-fighting (e.g.
counter-terrorism) to political purposes.

In the next subsection, I will discuss how politics and factionalism within the ZDF affect every-
day surveillance practices.
Politics, factionalism and quotidian surveillance practices within the ZDF

Everyday politics and factionalism within and without the ZDF influence military-driven surveillance. I will begin with politics outside the ZDF. As I argued at the start of this article, the ZDF has become an instrument for retaining power for the ruling ZANU-PF party. For the ZDF to successfully aid ZANU-PF’s quest for political hegemony, military-driven surveillance must be protected from the prying eyes of CSOs, activists and opposition MPs in the House of Assembly. This is where ZANU-PF comes in. The ruling party uses its dominance in the House of Assembly to shield the ZDF. First, the Defence, Home Affairs and Security portfolio committee is dominated by ZANU-PF legislators. Out of its 12 members, ten are ruling-party legislators, and of those ten, eight are former soldiers. This is where the symbiosis sets in. The committee shields the military from any legislation or operational scrutiny. As one respondent noted, ‘ZANU-PF will make sure that discussion around the operations of the ZDF do [sic] not stray into two areas – the ZDF budget and its internal operations’ (Interview 1). Opposition MPs have raised the issues of the military’s budget and operations several times, but ZANU-PF uses its dominance to brush them aside (Interview 5). The Zimbabwe Coalition on Debt and Development (ZIMCODD) has on several occasions raised red flags about the ZDF’s murky budgetary spending allocation. For instance, it notes that the ZDF receives a huge budget from the national treasury. It then receives funds loosely designated as operational funds. In addition, the office of the president also channels funds to the ZDF. Added to these are state-guaranteed grants offered by other militaries, such as the Red Army of the communist People’s Republic of China (ZIMCODD, 2020). With all these resources at its disposal, and with no parliamentary oversight, the ZDF is able to pursue surveillance unhindered. This explains why ZANU-PF will never cede parliamentary oversight to opposition MPs. After all, controlling the Defence, Home Affairs and Security portfolio is as good as controlling the ruling party itself. However, the caveat is that if civilian institutions fail to exercise control over the military, the latter can go rogue, and this imperils democracy. One respondent noted, ‘We never reported to Parliament. The view within the ZDF is that military issues are not civilian. We had interacted with Parliament, but not the kind of interaction you can define as proper accounting’ (Interview 9). Another respondent noted that they would ‘pass heavily truncated documents to Parliament with no meaning at all . . . just to go through the motions of reporting and placate voices agitating for accountability . . . but we knew nothing could be understood from the documents as real information is removed . . . and when we presented ourselves to the committee . . . we never discussed the real issues, and such questions were never asked’ (Interview 6). Because surveillance has become rhizomatic at all levels of its practice, effective oversight is now a challenge. It is difficult for CSOs, activists and statutory bodies like parliamentary committees to ensure effective oversight that would ensure that the ZDF does not interfere in or influence party political competition and that it sticks to its constitutional mandate of safeguarding security in the country if in fact these organizations have no clear picture of the military’s murky practices.

Politics within the ZDF itself also influence digital surveillance. Politics have always been part of the ZDF’s history (Tendi, 2020). But the internal politics of the ZDF became manifest after the year 2000. As the ruling party tottered under the weight of a formidable opposition and economic collapse, senior military commanders began to align themselves with factional sides within ZANU-PF. The hardliners, who had the dominant support within ZANU-PF, borrowed heavily from ZANU-PF’s political framing of national security discourse as an absolute value. National security discourses trumped other considerations like human rights and privacy. This normalizes surveillance. The dominant narrative among the political elites is that the country is under siege from a Western-sponsored opposition party and civil society organizations clamouring for regime change. The military should therefore mobilize all of the ZDF’s capabilities to defend the state...
from the British and the Americans. This political narrative seeking to justify and normalize military-driven surveillance is a bold attempt by both the military and the ruling party to ‘apply lipstick on a frog’ (*Newsday*, 2020). *Newsday* is a neoliberal and pro–human rights news outlet whose views would generally be the opposite of those of Zimbabwe’s conservative ruling class. The political elites’ reasoning is simply not backed by facts. Since its independence in 1980, Zimbabwe has never suffered a significant military threat, either internal or external, that would warrant practical mobilization of its armed forces to a level at which even the military’s surveillance apparatus was extensively mobilized. Murky and constitutionally unsupported, military surveillance confirms the ZDF’s ‘oversight allergy’ – that is, its aversion to civilian oversight.

Factionalism within the ZDF also colors the practice of digital surveillance. The ZDF has never been a unified entity (Rupiya, 2013). But factionalism within the institution increased in the twilight of Robert Mugabe’s regime and in the contemporary ‘Second Republic’. The coup that toppled former leader Mugabe in 2017 was in fact an ultimate violent explosion of this factionalism. The same factionalism has shaped military-driven surveillance in terms of widening the targets of surveillance. Respondents noted that while the main targets of the military’s surveillance practices are all those exterior forces ranged against ZANU-PF’s rule, factionalism within the military has ensured that ‘senior commanders of the ZDF and elite politicians within the ruling party are also targeted for surveillance’ (Interview 2). Some of these commanders, according to respondents, ‘now live in perpetual fear because they are aware that surveillance is being practised on them’ (Interview 2). As a result of factionalism, therefore, surveillance reflects the suspicions within the ruling party itself. Factionalism in the ZDF has always been an issue of political loyalty.

Political loyalty is fluid, however, especially if it is dictated by other self-interests, which in the case of the ZDF senior command involve the accumulation of material wealth and political self-aggrandizement (Makumbe, 2009). For such accumulation to happen, ZANU-PF rule must be perpetual, and every senior member of the military elite must be in the right faction. Accordingly, each faction uses surveillance tools, not only for the broader and shared objective of political policing on behalf of ZANU-PF, but also to manipulate the political process within ZANU-PF itself by outfoxing other factions using surveillance data gathered within the military apparatus. As one respondent noted, ‘The military surveillance practices intensified after the fall of Mugabe. With various factions jostling for power and influence . . . you will see that even senior ruling-party officials become targets . . . and many military figures’ (Interview 4). I argue that factionalized military-driven surveillance is a form of ‘political entrepreneurship’, where actors who should act on behalf of non-partisan goals of the state use their skills, power and influence in partisan political activities to gain power on their own behalf. Because it rarely engages with other civilian institutions mandated constitutionally to practise surveillance, the military robs itself of the opportunity to cross-pollinate ideas and share experiences with such institutions. Such shared experiences might improve the military’s own practices. But this would only be the case if the military’s surveillance were aimed at the broad objective of national security, not the current scenario in which it is merely a practice for maintaining power by identifying and neutralizing domestic opponents.

This makes the practice antithetical to modern-day democratic practices in that it serves political rather than state interests. Schedler (2002) argues that semi-authoritarian regimes manipulate four zones of public life – the electoral field, the judiciary, the legislature and the media – for political survival and hegemony. The case of the ZDF articulated here calls for the addition of military-driven surveillance to these four zones of contestation. Semi-authoritarian regimes make attempts to abide by available laws to provide a veneer of legality (Levitsky and Way, 2003). The military-driven surveillance system of Zimbabwe’s semi-authoritarianism, however, is a negation of Levitsky and Way’s assertion because it is an unrestrained constitutional aberration. Consequently, semi-authoritarianism should be understood differently, as rules are not often followed even to
maintain a veneer of legality. The Zimbabwean case of military-driven surveillance is exacerbated by two factors: first, the absence of grassroots civilian movements, an independent legislature and an independent judiciary that might help limit the military’s involvement in internal security matters; and, second, the growing unregulated global trade in surveillance technology, especially the current shift that seems to have favoured Chinese technology companies in Africa. It is to this second factor that I now turn.

**The political economy of surveillance technology acquisition: The role of China**

We must understand the global political economy of surveillance technology acquisition if we are to understand the growing practice of military-driven digital surveillance in Zimbabwe. There is a growing and complex global ‘surveillance industrial complex’ (Ball and Snider, 2013: 12) rooted in a global competition for control of the surveillance technology market. This industrial complex entangles actors such as militaries, surveillance technology corporations and elite politicians who make acquisition decisions. For the ZDF, there is an assorted mixture of enablers that include China, Iran and Russia (CIPESA, 2016). China, Iran and Russia have been jostling to be the main suppliers, not only of surveillance technology, but also of weapons and other military hardware to Zimbabwe (*Christian Science Monitor*, 2012). These three countries are united by the fact that each has a dubious human rights record (MPDP, 2019). It is the central role of China and its technology companies as suppliers that needs to be interrogated in this article. Technology companies involved include Huawei, ZTE and CloudWalk (MPDP, 2019). As one respondent noted, ‘We cannot talk of military surveillance without talking about China and its technology companies. . . . China and its technology companies sustain ZDF’s surveillance practices by readily supplying the equipment’ (Interview 7). Why does the ZDF look to China for its surveillance technology? What specific needs do Chinese surveillance technologies provide? These questions require interrogation. I should, however, emphasize that the absence of relevant human and technological expertise in Zimbabwe has always been a reason why technology has been sourced from without and why the Chinese have been asked on many occasions to ‘collaborate with ZDF in building human resources capabilities’ (MPDP, 2019: 11). The Zimbabwean case exemplifies the ‘Beijingification’ of the global industrial complex of surveillance. It also illustrates the agency of military actors as acquirers of surveillance technology at the global level.

Under the notion of the ‘Beijingification’ of digital surveillance, I refer to four surveillance practices that I argue are uniquely from, or at least prominently inherited from, Beijing. The first of these is the encroachment of the military upon quotidian civilian surveillance practices, where the People’s Liberation Army of China is known for its centre-stage role in digital surveillance practices (Swaine, 1998). Second, ‘Beijingification’ of surveillance means the appropriation of private, profit-making technology companies like ZTE and Huawei to push the ideology of the ruling Communist Party of China (CCP). This blurs the difference between these technology companies as profit-making entities and as instruments of the ruling party’s surveillance architecture, as they become part of the CCP’s global strategic defence and foreign policy apparatus. Third is the rampant and ‘normalized’ use of surveillance technologies by the ruling elite for monitoring purposes, especially of opposition supporters and any other forms of legitimate dissent. Lastly comes the use of digital surveillance technology to surveil internal political dissent within the ruling party itself. The Chinese government has succeeded in pursuing ‘hard authoritarianism’ characterized by blanket and banal surveillance but tempered by economic growth and development. The Zimbabwean government has not been able to replicate China’s economic success. Thus, its surveillance practices, while closely replicating the Chinese model, have not been strengthened by economic incentives, as in China. This leaves military-driven digital surveillance in Zimbabwe as the major weapon in the arsenal of the ruling party for forestalling civil unrest and dissent.
To understand China’s involvement in Zimbabwe, we need to understand Zimbabwe’s international relations, especially its relations with the West, as well as Beijing’s own intentions. Since its initiation of a violent program of land reform and the violence of the 2000 elections (see Sachikonye, 2011), Zimbabwe has had strained relations with the West and the USA, and has been slapped with sanctions that have made it impossible for it to purchase security-related equipment from companies domiciled in the West. Western companies are severely restricted from trading with Zimbabwe in military and security-related technologies. This has left the country with no option but to look east. As one respondent noted, ‘Western companies do hesitate to deal with the ZDF in this regard . . . and certainly Chinese companies are very comfortable dealing with the ZDF’ (Interview 4). Western-based companies are most likely to ask end-user questions when security-related technology is purchased. The ZDF ‘is not comfortable with questions about how they would be using the technology . . . those are very uncomfortable questions’ (Hawkins, 2018). The Chinese government and Chinese technology manufacturers have no human rights threshold to consider when supplying such technology (Hawkins, 2018). Furthermore, the secrecy of purchases cannot be guaranteed when sensitive equipment is purchased from Western-based corporations. One respondent agreed, ‘There is [Freedom of Information] requests very much alive especially in Europe. A company may be requested to disclose who purchased its equipment . . . They know they will find their names all over media’ (Interview 9). The ZDF is already aware of its tattered global image as a politicized institution abused by ZANU-PF for political policing (Sachikonye, 2011). Avoiding further controversies associated with the purchase of surveillance equipment is in its best interests.

Furthermore, to situate Chinese involvement, we need to understand policymaking in Zimbabwe’s elite spheres. Policymaking is not domiciled within the ZDF (Rupiya, 2013). It lies within the domain of non-military elites in cabinet positions (Rupiya, 2013). In line with existing foreign policy objectives, these determine who supplies what to the ZDF. Thus, even if the practical limitations of Chinese surveillance technologies are noticed, the military has no ultimate say on whom to engage. We now observe the emergence of a closely-knit military (ZDF) and Chinese surveillance industrial complex that sees Chinese technology companies benefitting financially from the increased acquisition of surveillance equipment. As one respondent noted, ‘The Chinese have made acquisition of surveillance equipment very easy . . . The ZDF sees this as a great advantage, as they can pay later’ (Interview 6).

Zimbabwe provides an experimental ground on which new surveillance technologies can be trained. Hawkins (2018) notes the facial recognition technology innovation by Chinese companies, which ‘requires black faces’ to make it efficient. Thus, Zimbabweans might now be ‘technology’s guinea pigs’. Recent research has shown that Chinese technology companies are not only exporting their digital surveillance technologies but also using the destination countries of their exports as training grounds to test and sharpen their technologies. Romaniuk and Burgers (2018) note that ZTE, for instance, has exported surveillance cameras to Ethiopia and simultaneously tested some of its technologies in the country. Andersen (2020) notes that Chinese technology companies have exported technology used by Malaysian police, tested their surveillance algorithms technology in wider East Asia, and tested some of the equipment in Malaysia itself. Andersen (2020) further asserts that Beijing is using its exports to Asia and Africa to innovate and sharpen new surveillance technologies, which it will then export to other contexts or use at home. On Chinese companies using Zimbabwe for testing surveillance technology, Hawkins (2018) notes how the deal between the Zimbabwean government and the Chinese company CloudWalk is working:

And by gaining access to a population with a racial mix far different from China’s, CloudWalk will be better able to train racial biases out of its facial recognition systems – a problem that has beleaguered facial recognition companies around the world and which could give China a vital edge.
Thus, the cases of Malaysia, Ethiopia and Zimbabwe outlined above show how research, development and technology testing are central to China’s broader design and intentions in relation to surveillance. China’s intentions are being advanced through importing companies. Two factors make it easy for Chinese companies to experiment with surveillance data from Zimbabwe: there is no law in Zimbabwe’s legislation that provides for how data held by state agencies are to be used or disposed of, and there is no rule regulating military surveillance in civilian spaces. Therefore, the data can be utilized surreptitiously to sharpen Chinese surveillance technologies.

By supplying surveillance technologies to the ZDF, China and its companies now shape Zimbabwe’s surveillance policies and strategies, most likely in ways that mimic those of China. China’s surveillance practices are notoriously opaque, authoritarian, invasive of privacy, extra-legal and military in nature (Hawkins, 2018). As I demonstrate here, Zimbabwe’s military-driven surveillance drifts along similar lines. Mimicking China’s surveillance practices would not only strengthen the Chinese position in the country but also might lead to a notoriously hard form of (Chinese) rhizomatic surveillance culture. The Zimbabwean military might experiment with this emerging form of surveillance with the help of Chinese companies and the Beijing government itself, as the latter spreads its surveillance tentacles throughout the African continent. Some scholars (e.g. Gagliardone, 2020) have argued, however, that some forms of surveillance may not be replicable in non-Chinese political, social and economic contexts. After all, Chinese technology companies – like their Western and US-based counterparts such as Ericsson, Facebook and Google – just seek profits and lucrative business. Moreover, these Chinese companies employ their own skilled workforces made up of individuals seeking better economic opportunities abroad.

Research carried out by MPDP (2019) would appear to favour such a view, emphasizing that, no matter how large the surveillance ambitions of the ZDF may be, a financially bankrupt state will not be able to fund these ambitions in the long run. But such arguments seriously misread the Zimbabwean case. They are based on the erroneous view that Zimbabwe’s political leadership runs a transparent regime. The massive investment in Chinese technology within the ZDF’s surveillance architecture, together with Beijing’s own investments, illustrates the intimate and instrumental ties between China and the ZDF. Also, China’s geopolitical ambitions should not be underestimated. Beijing will go a long way to appease allies – not out of ‘Chinese benevolence’ but in accordance with long-term geopolitical goals of competing with the West and the USA in Africa. The Zimbabwe Coalition on Debt and Development has noted that the ZDF already has huge amounts of undisclosed debts to China (ZIMCODD, 2020). Thus, the mafiarism and opaque nature of the ruling regime will allow it to pump more resources into enabling the ZDF’s surveillance capabilities, with little accountability, and in the process safeguarding the ruling regime’s own political survival.

**Discussion and conclusions**

There is a connection between the widening practice of military-driven digital surveillance in Zimbabwe and the political survival of the country’s ruling party ZANU-PF. The real threat posed by opposition groups and the regime’s own governance failures make surveillance a preferred tool of political control. In this article, I have argued that the politicization of the ZDF as a security institution enables it to bolster and reproduce ZANU-PF’s political dominance of the state. I have further argued that political factionalism within the ZDF has provided for rhizomatic flows of surveillance technology and practices, along with numerous other forms of military-driven digital surveillance – for example, the surveillance of senior ruling-party and military elites. For surveillant-assemblage theorists, the ZDF case demonstrates in acute fashion the ‘authoritarianization’ of the surveillant assemblage, where surveillance technology is increasingly being appropriated around the solidification of political monitoring and profiling of legitimate opponents. It thus
illustrates how the surveillant assemblage is shaped in semi-authoritarian regimes in ways that neatly dovetail with support for hegemonic political parties. Accordingly, in semi-authoritarian regimes, the surveillant assemblage should be understood as a weapon configured in a broader field of political contestation pitting a hegemonic political party on the verge of losing power and legitimate opponents on the cusp of gaining it.

My argument illustrates the phenomenon of the ‘surveillance paradox’. The ZDF’s surveillance practices are paradoxical in the sense that while ZANU-PF and the military largely benefit from such practices, the political factionalization of the ZDF has made them victims of the very same practices that were intended to benefit them. This paradox is likely to be a defining feature of military-driven surveillance beyond the present case of Zimbabwe, where semi-authoritarian regimes appropriate the military for the purpose of political survival. The victimizer often becomes the victim. The Zimbabwean case therefore exhibits a levelling effect (Haggerty and Ericson, 2000): even within the military itself, some of its own elements are targeted for surveillance. Thus, at the centre of the ZDF’s surveillance tactics and the circulation of the surveillance technologies themselves lies political loyalty to ZANU-PF, which trumps every practical consideration because it guarantees the survival of the ZDF in its current politicized form.

The continued militarization of civilian spaces through surveillance has led to the attenuation of civilian institutions. For instance, the role of the CIO and the ZRP, which have constitutional mandates under the Information and Communication Act to carry out digital surveillance for criminal investigations, is gradually being eclipsed by the military’s mission creep. Over the years, the army has expanded rapidly and has enlisted large numbers of poorly schooled people who lack the basic skills and character necessary to become efficient and disciplined security enforcers. It is impossible that such a crop of security officers can adjudicate non-politically in the sensitive field of surveillance. The situation here is different from that of other military-driven, semi-authoritarian surveillance contexts, such as that of Myanmar. The surveillance practices of Myanmar’s military thrive on a carefully managed policy of recruiting tech-savvy individuals who are fiercely loyal to the Tatmadaw (Duncan and Mendelson, 2021).

There are policy-specific dangers associated with continued military-driven surveillance, especially in Zimbabwe, where state institutions are too weak to check the military’s expansion. One of these is the ‘rub-off effect’ of military-driven surveillance. By their nature, the tools, tactics and attitudes of the military are not meant to be applied to civilians, but to the military’s combat opponents (German, 2014). Even the military’s surveillance technologies naturally differ from those of civilian (supposedly crime-related) surveillance. If, as the Zimbabwean case shows, the military drives surveillance practices and comes into interaction with civilian-trained surveillance personnel, the latter may well end up copying military practices. Military-driven surveillance often avoids the law and is contemptuous of the truth (German, 2014). Thus, civilian surveillance institutions may also end up being contemptuous of the law and treat civilians as enemy combatants. Within the military itself, a cynical view might be inculcated that the most expedient route to solving political and social dissent is through military-style surveillance. Such a view endangers democracy and is detrimental to fundamental individual liberties such as the right to dissent.

This article has added to the small amount of existing research on military-driven surveillance practices by exploring the phenomenon of military-driven surveillance within a semi-authoritarian political system that has been the subject of relatively little study. It has made a contribution to the literature on emerging forms of militaristic politics that thrive on the conscription of surveillance into quotidian civilian life, in which digital surveillance technologies become tools of repression and control. The Zimbabwean case demonstrates the dangers to democracy of the militarization of legitimate political conflict between a ruling party and its opposition. Such a development wrecks not only the well-established concept of separation of powers but also popular clamours for
democracy, freedom and human rights that have always defined semi-authoritarian politics. The Zimbabwean case also has implications for global security. It demonstrates the need to introduce restrictions and to regulate the global coordination of trade in surveillance technologies. Surveillance technologies are the nuclear weapons of this century owing to the huge amount of data they yield and the possible political consequences of their use. If there is to be a continued nation-to-nation trade in surveillance technologies around the globe, it needs to be open and transparent. This would ensure that technology companies are held responsible for the ultimate use of their technologies. This would make Chinese technology companies, as in the Zimbabwean case, liable for sinister and undemocratic appropriation of their technologies. Such companies would thus be prevented from being purveyors of a global anti-democracy tide spurred on by digital surveillance. It would also prevent an undemocratic military-driven surveillance culture from diffusing at the global level, with incalculable risks for fundamental freedoms such as privacy – freedoms that are central to global collective security.

Acknowledgements
I would like to thank Professor Mark B. Salter for his insightful comments on the first draft of this article, which draws on research I conducted for MPDP, supported by Luminate, in 2020. I would like to thank the principal investigator of MPDP, Professor Jane Duncan of the University of Johannesburg, for allowing me space to conduct the research and an opportunity to coordinate the project.

Funding
The author received no financial support for the research, authorship, and/or publication of this article.

ORCID iD
Allen Munoriyarwa https://orcid.org/0000-0001-5064-3192

Notes
1. In the past, ZDF commanders frequently vowed to salute Robert Mugabe only; see Thornycroft and Butcher (2002).
2. An investigative report in NewsDay, one of the country’s most trusted daily newspapers, made detailed exposures; see Chingarande (2020).
3. The recent case of Job Sikhala, a vice-president of the opposition Movement for Democratic Change Alliance (MDCA), can be followed at New Zimbabwe (2020). The revelation of the military’s involvement was made publicly by a former cabinet minister; see https://twitter.com/profjnmooyo/status/1292544131080884226 (accessed 22 June 2022).

References
Andersen R (2020) The panopticon is already here. The Atlantic, September. Available at: https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/ (accessed 17 July 2021).
Ball K and Snider L (2013) The Surveillance-Industrial Complex. Abingdon: Routledge.
Basturk E (2017) A brief analyse on post panoptic surveillance: Deleuze&Guattarian approach. International Journal of Social Sciences 6(2): 1–17.
Berda Y (2013) Managing dangerous populations: Colonial legacies of security and surveillance. Sociological Forum 28(3): 627–630.
Chingarande D (2020) Securocrats scale up surveillance. NewsDay, 23 October. Available at: https://www.newsdays.co.zw/2020/10/securocrats-scale-up-surveillance/ (accessed 17 July 2021).
Christian Science Monitor (2012) Why Iran wants to beef up Zimbabwe’s military. 15 March. Available at: https://www.csmonitor.com/World/Africa/2012/0315/Why-Iran-wants-to-beef-up-Zimbabwe-s-military (accessed 12 September 2021).
Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (2016) State of the Cyberspace in Southern Africa. Mombasa: CIPESA.

Dandeker C (2006) Surveillance and military transformation: Organizational trends in twenty-first-century armed services. In: Haggerty KD and Ericson RV (eds) The New Politics of Surveillance and Visibility. Toronto: University of Toronto Press, 225–249.

Dempsey L, Dowling M, Larkin P and Murphy K (2016) Sensitive interviewing in qualitative research. Research in Nursing & Health 39(6): 480–490.

Duncan K and Mendelson A (2021) The Tatmadaw has mass surveillance technology, but how well is it used? Globe, 7 June. Available at: https://southeastasiaglobe.com/myanmar-military-surveillance/ (accessed 14 October 2021).

Enosh G and Buchbinder E (2005) Strategies of distancing from emotional experience: Making memories of domestic violence. Qualitative Social Work 4(1): 9–32.

Gagliardone I (2020) The impact of Chinese tech provision on civil liberties in Africa. SAIIA Policy Insights no. 99. Available at: https://saiia.org.za/research/the-impact-of-chinese-tech-provision-on-civil-liberties-in-africa/ (accessed 14 June 2022).

German M (2014) The militarization of domestic surveillance is everyone’s problem. Brennan Center for Justice, 18 December. Available at: https://www.brennancenter.org/our-work/analysis-opinion/militarization-domestic-surveillance-everyones-problem?_ga=2.220514648.1742738142.1613402602-908828103.1613402602 (accessed 23 February 2021).

Gill P (2012) Policing Politics: Security Intelligence and the Liberal Democratic State. Abingdon: Routledge.

Global Times (2018) China exports facial ID technology to Zimbabwe. 13 May. Available at: https://www.globaltimes.cn/content/1097747.shtml (accessed 10 May 2020).

Greenberg I (2012) Surveillance in America: Critical Analysis of the FBI, 1920 to the Present. New York: Lexington Books.

Haggerty KD and Ericson RV (2000) The surveillant assemblage. The British Journal of Sociology 51(4): 605–622.

Hagmann J (2021) Globalizing control research: The politics of urban security in and beyond the Alaouite Kingdom of Morocco. Journal of Global Security Studies 6(4): ogab004.

Hawkins A (2018) Beijing’s Big Brother tech needs African faces: Zimbabwe is signing up for China’s surveillance state, but its citizens will pay the price. Foreign Policy, 24 July. Available at: https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ (accessed 13 August 2020).

Howell A (2018) Forget ‘militarization’: Race, disability and the ‘martial politics’ of the police and of the university. International Feminist Journal of Politics 20(2): 117–136.

Jensen JM (1991) Army Surveillance in America, 1775–1980. New Haven, CT: Yale University Press.

Levitsky S and Way LA (2003) Ties that bind? International linkage and competitive authoritarian regime change in Africa, Latin America, and post-communist Eurasia. Paper prepared for the Annual Meeting of the American Political Science Association, Philadelphia, PA, 27–30 August 2003.

Lyon D (2006) Surveillance After September 11. Montreal: Polity Press.

Magaisa A (2019) Zimbabwe: An opportunity lost. Journal of Democracy 30(1): 143–157.

McMichael C (2017) Pacification and police: A critique of the police militarization thesis. Capital & Class 41(1): 115–132.

Makumbe J (2009) The Impact of Democracy in Zimbabwe: Assessing Political, Social and Economic Developments Since the Dawn of Democracy. Harare: University of Zimbabwe Publishers.

Masunungure E (2011) Zimbabwe’s militarized, electoral authoritarianism. Journal of International Affairs 65(1): 47–64.

Media Policy and Democracy Project (MPDP) (2019) Drifting towards darkness: An exploratory research of state surveillance in post-2000 Zimbabwe. Available at: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/zimbabwe_report_2nd_pages.pdf (accessed 20 July 2020).

Nagy V (2017) How to silence the lambs? Constructing authoritarian governance in post-transitional Hungary. Surveillance & Society 15(3/4): 447–455.

Ndlela D (2020) Military surveillance could endanger democracy. NewsDay, 19 March. Available at: https://www.newsday.co.zw/2020/03/military-surveillance-could-endanger-democracy/ (accessed 20 June 2022).
New Zimbabwe (2020) ‘#July31: Police Hunt For Sikhala, Godfrey Tsenengamu, 11 Activists’. 28 July. Available at: https://www.newzimbabwe.com/july31-police-hunt-for-sikhala-godfrey-tsenengamu-11-activists/ (accessed 11 August 2021).

Neocleous M (2015) War Power, Police Power. Edinburgh: Edinburgh University Press.

Newday (2020) Army’s social media snooping bone-chilling. 5 March. Available at: https://www.newday.co.zw/2020/03/armys-social-media-snooping-bone-chilling/ (accessed 12 September 2021).

Noyes AH (2018) A new Zimbabwe: Assessing continuity and change after Mugabe. Presentation at the Rand Arroyo Center, Santa Monica, CA, 27 September.

Ogasawara M (2019) Mainstreaming colonial experiences in surveillance studies. Surveillance & Society 17(5): 726–729.

Ottaway M (2003) Democracy Challenged: The Rise of Semi-Authoritarianism. Washington, DC: Carnegie Endowment for International Peace.

Romaniuk S and Burgers T (2018) How China’s AI technology exports are seeding surveillance societies globally. The Diplomat, 18 October. Available at: https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/ (accessed 14 June 2022).

Ruhanya P (2018) Militarisation of state institutions and the November military coup. Zimbabwe Independent, 17 November. Available at: www.theindependent.co.zw-of-state-institutions-and-the-november-military-coup (accessed 14 June 2022).

Rupiya M (2013) The military factor in Zimbabwe’s political and electoral affairs. SW Radio Africa. Available at: http://www.swradioafrica.com/Documents/The%20Military%20Factor%20in%20Zimbabwe.pdf (accessed 17 July 2021).

Sachikonye L (2011) When a State Turns on Its Citizens: 60 Years of Institutionalised Violence in Zimbabwe. Harare: Weaver Press.

Schedler A (2002) Elections without democracy: The menu of manipulation. Journal of Democracy 13(2): 36–50.

Seigel M (2018) Violence work: Policing and power. Race & Class 59(4): 15–33.

Standard (2020a) Creating a surveillance state: ED govt zooms in for critics with Chinese. 1 March. Available at: https://www.thestandard.co.zw/2020/03/01/creating-surveillance-state-ed-govt-zooms-critics-chinese-help/ (accessed 14 September 2021).

Standard (2020b) ‘Zim’s era of the state’ could herald increased repression. 6 September. Available at: https://www.thestandard.co.zw/2020/09/06/zims-era-of-the-state-could-herald-increased-repression/ (accessed 20 June 2022).

Swaine MD (1998) The Role of the Chinese Military in National Security Policymaking, rev. edn. Santa Monica, CA: RAND Corporation. Available at: https://www.rand.org/pubs/monograph_reports/MR782-1.html (accessed 12 September 2021).

Taruvinga M (2019) Zimbabwe: High Court orders release of slain CIO operative’s post-mortem report. NewZimbabwe.com, 23 May. Available at: https://allafrica.com/stories/201905230594.html (accessed 20 June 2022).

Tendi BM (2020) The motivations and dynamics of Zimbabwe’s 2017 military coup. African Affairs 119(474): 39–67.

Thornycroft P and Butcher T (2002) Military ‘will not accept Mugabe defeat’. Telegraph, 10 January. Available at: https://www.telegraph.co.uk/news/worldnews/africaandindianocean/zimbabwe/1381018/Military-will-not-accept-Mugabe-defeat.html (accessed 14 June 2022).

Wilson D (2012) Military surveillance. In: Ball K, Lyon D and Haggerty KD (eds) Routledge Handbook of Surveillance Studies. Abingdon: Routledge, 269–277.

Yonucu D (2018) Urban vigilantism: A study of anti-terror law, politics and policing in Istanbul. International Journal of Urban and Regional Research 42(3): 408–422.

Zimbabwe Coalition on Debt and Development (ZIMCODD) (2020) Zimbabwe Coalition on Debt and Development: Second Quarter Report. Available at: https://zimcodd.org/wp-content/uploads/2020/03/ZIMCODD-2nd-Quarter-Report.pdf (accessed 14 September 2021).
Interviews cited

1. Former officer, Special Investigative Unit, Zimbabwe National Army
2. Former member, Special Investigative Unit, Zimbabwe National Army
3. Former member, Signals Unit, Zimbabwe National Army
4. Former member, Zimbabwe Military Police
5. Former ZANU-PF member of Defence and Foreign Affairs Committee
6. Former member, Signals Unit, Zimbabwe National Army
7. Former member, Special Investigative Unit, Zimbabwe National Army
8. Former instructor, Military College
9. Former member, Zimbabwe Military Police

Allen Munoriyarwa is a senior post-doctoral research fellow in the Communication and Media Department at the University of Johannesburg. He is also affiliated to the Centre for Data and Digital Technologies in the School of Communication at the University of Johannesburg. His research interests are journalism, news production practices, big data and digital surveillance. He is currently coordinating research on digital surveillance practices in Southern Africa under the auspices of the Media Policy and Democracy Project. Email: allenmunoriyarwa@gmail.com.